W. NARKIEWICZ

Elementary and Analytic Theory of Algebraic Numbers

Third Edition

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(\frac{1}{1 - N(\mathfrak{p})^{-s}} \right)$$

Springer Monographs in Mathematics

Springer

Springer Monographs in Mathematics

Springer-Verlag Berlin Heidelberg GmbH

Władysław Narkiewicz

Elementary and Analytic Theory of Algebraic Numbers

Third Edition

Springer

Władysław Narkiewicz
Wrocław University
Institute of Mathematics
Pl. Grunwaldzki 2/4
50-384 Wrocław
Poland
e-mail: narkiew@math.uni.wroc.pl

Third, revised and extended edition based on the second edition (English):
© PWN-Polish Scientific Publishers, Warszawa 1990

Mathematics Subject Classification (2000):
11Rxx, 11Sxx

ISSN 1439-7382

ISBN 978-3-642-06010-6 ISBN 978-3-662-07001-7 (eBook)
DOI 10.1007/978-3-662-07001-7

Library of Congress Control Number: 2004105720

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag Berlin Heidelberg GmbH.
Violations are liable to prosecution under the German Copyright Law.

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Originally published by Springer-Verlag Berlin Heidelberg New York in 2004
Softcover reprint of the hardcover 3rd edition 2004
The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typeset in TEX by the author
Final typesetting: LE-TEX, Leipzig
Cover design: Erich Kirchner, Heidelberg

Printed on acid-free paper SPIN: 10941041 41/3141/ba - 5 4 3 2 1 0

To my wife

Preface

The aim of this book is to present an exposition of the theory of algebraic numbers, excluding class-field theory and its consequences. There are many ways to develop this subject; the latest trend is to neglect the classical Dedekind theory of ideals in favour of local methods. However, for numerical computations, necessary for applications of algebraic numbers to other areas of number theory, the old approach seems more suitable, although its exposition is obviously longer. On the other hand the local approach is more powerful for analytical purposes, as demonstrated in Tate's thesis. Thus the author has tried to reconcile the two approaches, presenting a self-contained exposition of the classical standpoint in the first four chapters, and then turning to local methods.

In the first chapter we present the necessary tools from the theory of Dedekind domains and valuation theory, including the structure of finitely generated modules over Dedekind domains. In Chapters 2, 3 and 4 the classical theory of algebraic numbers is developed. Chapter 5 contains the fundamental notions of the theory of $\mathfrak{p}$-adic fields, and Chapter 6 brings their applications to the study of algebraic number fields. We include here Shafarevich's proof of the Kronecker-Weber theorem, and also the main properties of adeles and ideles.

In Chapter 7 we apply analytical methods, and derive functional equations for various zeta-functions, including Dedekind zeta-functions and Dirichlet's L-functions. These functions are then applied to the study of asymptotic distributions of ideals and prime ideals. In Chapter 8 we consider Abelian extensions of the rationals. We prove the Siegel-Brauer theorem in this case, obtain the class-number formula, and give an effective bound for negative quadratic discriminants with class-number one. The last chapter deals with factorization of algebraic integers into irreducibles.

Each chapter ends with a section containing comments and a short review of the relevant literature. A short selection of exercises is also given.

At the end of the book we present a choice of open problems containing some classical questions, and also some problems of more recent vintage. In the first edition this list contained 35 problems, 14 were added in the second edition, and now we added 10 more. Some of them were solved in the meantime. They are marked by an asterisk in our list.

We expect the reader to have an elementary knowledge of algebraic and topological notions, including elements of Galois theory.

There are three appendices dealing with locally compact Abelian groups, Dirichlet series and Baker's method, presenting results utilized in the main text.

The comments at the end of each chapter have been rewritten to take account of the development of the subject up to 2003, and the bibliography has been extended accordingly. To keep the size of the book reasonable some changes in the main text have been made in comparison to the previous editions. Certain proofs were simplified, and we decided to omit a few theorems. In contrast to the previous editions, written on a typewriter, this time a computer was used, and this gave the possibility to improve the text on several places. I am grateful to several friends and colleagues, who commented on the previous editions. A particular thank goes to Dr.Tadeusz Pezda, who carefully read the outprints of the new version, and suggested several clarifications and improvements.

Finally I would like to thank the Springer Verlag for the cooperation in the realization of this book.

Wrocław, January 2004 Władysław Narkiewicz

Table of Contents

Notation XI

1. Dedekind Domains and Valuations 1

1.1. Dedekind Domains 1
1.2. Valuations and Exponents 16
1.3. Finitely Generated Modules over Dedekind Domains 24
1.4. Notes to Chapter 1 37
Exercises 40

2. Algebraic Numbers and Integers 43

2.1. Distribution of Integers in the Complex Plane 43
2.2. Discriminants and Integral Bases 52
2.3. Applications of Minkowski'e Convex Body Theorem 66
2.4. Notes to Chapter 2 69
Exercises 82

3. Units and Ideal Classes 85

3.1. Valuations of Algebraic Number Fields 85
3.2. Ideal Classes 92
3.3. Units 96
3.4. Euclidean Algorithm 115
3.5. Notes to Chapter 3 119
Exercises 132

4. Extensions 135

4.1. The Homomorphisms of Injection and Norm 135
4.2. Different and Discriminant 146
4.3. Factorization of Prime Ideals in Extensions. More about the Class Group 167
4.4. Notes to Chapter 4 185
Exercises 196

5. $\mathfrak{P}$-adic Fields 199
5.1. Principal Properties 199
5.2. Extensions of $\mathfrak{p}$-adic Fields 221
5.3. Harmonic Analysis in $\mathfrak{p}$-adic Fields 237
5.4. Notes to Chapter 5 250
Exercises 254

6. Applications of the Theory of $\mathfrak{P}$-adic Fields 257
6.1 Arithmetical Applications 257
6.2. Adeles and Ideles 286
6.3. Notes to Chapter 6 307
Exercises 312

7. Analytical Methods 313
7.1. The Classical Zeta-Functions 313
7.2. Asymptotic Distribution of Ideals and Prime Ideals 343
7.3. Chebotarev's Theorem 364
7.4. Notes to Chapter 7 389
Exercises 405

8. Abelian Fields 409
8.1. Main Properties 409
8.2. The Class-number Formula and the Siegel-Brauer Theorem 423
8.3. Class-number of Quadratic Fields 436
8.4. Notes to Chapter 8 459
Exercises 482

9. Factorizations 485
9.1. Elementary Approach 485
9.2. Quantitative results 496
9.3. Notes to Chapter 9. 507
Exercises 509

Appendix I. Locally Compact Abelian Groups 511

Appendix II. Function Theory 525

Appendix III. Baker's Method 527

Problems 529

References 535

Author Index 685

Subject Index 701

List of Symbols 707

Notation

We shall use the following standard notation:

The letter $\mathbb{C}$ will denote the complex field, $\mathbb{R}$ the field of real numbers, $\mathbb{Q}$ the field of rationals, $\mathbb{Z}$ the ring of all rational integers, $\mathbb{N}$ the set of all positive integers and $\mathbb{P}$ the set of all rational primes. F_q will denote the finite field of q elements. By $[x]$ and $\{x\}$ we shall denote the integral resp. fractional part of x.

The letter p with or without indices will be reserved for prime numbers, except when explicitly stated. For prime p the notation $p^a \parallel n$ means that p^a is the largest power of p dividing n. The cardinality of a set A will be denoted by $\#A$.

The m-th primitive root of unity will be denoted by ζ_m. In fields of zero characteristic we shall assume $\zeta_m = \exp(2\pi i/m)$.

By $A \sim B$ we shall indicate that two algebraic structures A and B are isomorphic.

We shall use the Kronecker symbol δ_i^j defined by

$$\delta_i^j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

and the sign of a real number α will be denoted by $\operatorname{sgn} a$.

By *GRH* we shall mean the General Riemann Hypothesis (called sometimes the Extended Riemann Hypothesis), which states, that all zeros of zeta-functions of Riemann, Dedekind, and Hecke in the strip $0 < \operatorname{Re} s < 1$ lie on the line $\operatorname{Re} s = 1/2$.

The symbol $\square$ will indicate the end of a proof. Empty sums are considered to be equal 0, and empty products are equal 1.

1. Dedekind Domains and Valuations

1.1. Dedekind Domains

1. This chapter is introductory, and contains the fundamental properties of Dedekind domains including their behaviour under finite extensions and the structure of finitely generated modules. Moreover, we include elementary facts about valuations needed in the sequel.

Consider a commutative domain R, and let K be its field of quotients. Any non-zero R-module I contained in K, and such that for a certain non-zero $a \in R$ we have $aI \subset R$, will be called a *fractional ideal* of R. Every fractional ideal contained in R is an ideal in the usual sense, and the converse holds for all non-zero ideals. If I_1, I_2 are fractional ideals, then their *product* $I_1 I_2$ is defined as the set of all sums $a_1 b_1 + \cdots + a_m b_m$ with $a_i \in I_1$ and $b_i \in I_2$. This set is also a fractional ideal. Indeed, it is a non-zero R-module contained in K, and if $x, y \neq 0$ lie in R and satisfy $xI_1 \subset R$, $yI_2 \subset R$, then for $\alpha = \sum_i a_i b_i$ in $I_1 I_2$ we get

$$(xy)\alpha = \sum_i (xa_i)(yb_i) \in R.$$

Observe that for a non-zero $a \in K$ the set aR is a fractional ideal. Such ideals are called *principal fractional ideals*. It is clear that the set of all fractional ideals of R forms a commutative semigroup with a unit element equal to R.

Any commutative ring with a unit element, but possibly with zero-divisors, is called a *Noetherian ring* if every ascending chain of distinct ideals is necessarily finite.

Proposition 1.1. *A commutative ring with a unit element is Noetherian if and only if every its ideal is finitely generated.*

Proof : Let R be Noetherian and assume that $I \subset R$ is an ideal which is not finitely generated. Select a non-zero element $x_1 \in I$ arbitrarily, and if the elements $x_1, x_2, \ldots, x_n$ are already selected, then choose for x_{n+1} any element of I not contained in the ideal $x_1 R + x_2 R + \cdots + x_n R$. Such a choice is possible because I is not finitely generated. This leads to an ascending chain $x_1 R$, $x_1 R + x_2 R, \ldots$, of distinct ideals, contrary to our assumption.

Conversely, let R be a ring in which every ideal is finitely generated, and consider any ascending chain $I_1 \subset I_2 \subset \ldots$ of its ideals. The union $\bigcup_{n=1}^{\infty} I_n$ is an ideal in R, and so has a finite set of generators. But this set must already lie in some I_n, which shows that our chain has at most n distinct terms. □

Corollary. *If every ideal of R is principal, then R is Noetherian, provided it is commutative and has a unit element.* □

We shall need also the notion of a Noetherian module. If R is a commutative ring with a unit element, then an R-module M is called a *Noetherian module* if every ascending chain of its submodules has only a finite number of distinct terms. In the same manner as in Proposition 1.1 one shows that an R-module is Noetherian if and only if every its submodule is finitely generated.

Proposition 1.2. *(i) The direct sum of a finite number of Noetherian modules is again a Noetherian module.*

(ii) A homomorphic image of a Noetherian module is again Noetherian.

Proof : We start with a simple lemma:

Lemma 1.3. *If M is a Noetherian R-module and the sequence*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0 \tag{1.1}$$

is exact (i.e., M_1 is a sub-R-module of M and $M_2 \sim M/M_1$), then the modules M_1 and M_2 are also Noetherian. Conversely, if there exists a sequence (1.1) *with Noetherian M_1, M_2, then M is Noetherian.*

Proof : Let M be Noetherian and let (1.1) be exact. As every submodule of M_1 is a submodule of M, the noetherianity of M_1 results. If $\{I_m\}$ is an infinite ascending chain of distinct submodules of M_2, then the reciprocal images of I_m in M form an infinite ascending chain of distinct submodules of M, contradicting our assumption.

Assume now M_1, M_2 to be Noetherian and (1.1) to be exact. Let $\{I_m\}$ be an ascending chain of submodules of M, and let J_m be the image of I_m in M_2. The sequence $\{J_m\}$ is ascending, thus for sufficiently large n we have $J_n = J_{n+1} = J_{n+2} = \ldots$, and similarly we obtain for $J'_m = I_m \cap M_1$ the equalities $J'_{n_1} = J'_{n_1+1} = \ldots$ for sufficiently large n_1. Put $N = \max\{n, n_1\}$ and let $r \geq N$. If $a \in I_r$, then for a certain $b \in I_N$ we have $a - b \in M_1$, whence

$$a - b \in I_r \cap M_1 \subset I_N,$$

and $a \in I_N$. Thus $I_r \subset I_N$, and the sequence $\{I_m\}$ has only finitely many distinct terms, which implies that M is Noetherian. □

To prove our proposition note that its part (ii) is already contained in the lemma, and (i) follows by induction owing to the observation that for any R-modules A and B the sequence

$$0 \longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0$$

is exact. □

Corollary. *A finitely generated module over a Noetherian ring R is Noetherian.*

Proof : Applying part (i) of the proposition we obtain that R^k is Noetherian for every positive integer k, and it remains to observe that every finitely generated R-module is a homomorphic image of R^k for a suitable k, and so part (ii) of the proposition is applicable. □

From now on we shall assume that R is a commutative domain, and by K we shall denote its field of fractions. If I is a fractional ideal of R, then we shall denote by I' the set

$$\{x \in K : \ xI \subset R\}.$$

Obviously I' is a non-zero R-module. Observe that it is a fractional ideal. In fact, if y is a non-zero element of I, and r is a non-zero element of R satisfying $ry \in R$, then ry lies in $R \cap I$, and for every $a \in I'$ we have $ary \in R$.

It is easy to see that $II' \subset R$. If for a fractional ideal I the equality $II' = R$ holds, then we say that I is *invertible*, and write I^{-1} instead of I'.

Proposition 1.4. *Every principal fractional ideal is invertible, and the set of all invertible fractional ideals forms a group under multiplication.*

Proof : If $I = aR$ with a non-zero $a \in K$, then evidently $I' = a^{-1}R$ and $II' = R$ follows. Now note that if for two fractional ideals I_1, I_2 the equality $I_1 I_2 = R$ holds, then they are both invertible and $I_2 = I_1^{-1}$. Indeed, we have $I_2 \subset I_1'$, thus $R = I_1 I_2 \subset I_1 I_1' \subset R$, hence $I_1 I_1' = R$, and we see that I_1 is invertible, and, moreover, $I_1' = I_1' R = I_1' I_1 I_2 = R I_2 = I_2$. This observation shows that if I, J are both invertible, then in view of $IJ(I^{-1}J^{-1}) = R$ we get the invertibility of IJ, and it remains to observe that $(I^{-1})^{-1} = I$. □

If a domain R is not a field, and every fractional ideal of R is invertible, then we say that R is a *Dedekind domain*. Since a finite domain is a field it follows that every Dedekind domain is infinite.

The first part of the last proposition implies that every principal ideal domain is Dedekind, and this applies in particular to the ring $\mathbb{Z}$ of rational integers. Two important properties of Dedekind domains are given by the following theorem:

Theorem 1.5. *If R is a Dedekind domain, then R is Noetherian, and every non-zero prime ideal of R is maximal.*

Proof : Let I be a non-zero ideal in R. In view of $II^{-1} = R$ there exist elements $a_i \in I$, $b_i \in I^{-1}$ $(i = 1, 2, \ldots, m)$ such that $\sum_{i=1}^{m} a_i b_i = 1$. If now $x \in I$, then $x = \sum_{i=1}^{m} (xb_i)a_i$ and $xb_i \in R$, whence I is generated, as an R-module, by the finite set $\{a_1, \ldots, a_m\}$, and the noetherianity of R follows.

Now let $\mathfrak{p}$ be a non-zero prime ideal in R, and let $\mathfrak{P}$ be a maximal ideal containing it. We have $\mathfrak{p}\mathfrak{P}^{-1} \subset \mathfrak{P}\mathfrak{P}^{-1} = R$, and so $\mathfrak{p}\mathfrak{P}^{-1}$ is an ideal of R. As $\mathfrak{p}\mathfrak{P}^{-1}\mathfrak{P} = \mathfrak{p}$, we must have either $\mathfrak{p}\mathfrak{P}^{-1} \subset \mathfrak{p}$ or $\mathfrak{P} \subset \mathfrak{p}$, because $\mathfrak{p}$ is a prime ideal. The first possibility leads to $\mathfrak{P}^{-1} \subset \mathfrak{p}^{-1}\mathfrak{p} = R$, which implies $\mathfrak{P}^{-1} = R$ and $\mathfrak{P} = R$, but this is not possible, hence the second possibility must hold, and it leads to $\mathfrak{p} = \mathfrak{P}$. □

2. To obtain further results on Dedekind domains we have to introduce the notion of integrality. Let R be a domain, and let L be any field containing R (there is no need for L to coincide with the field of fractions of R). An element $x \in L$ is said to be *integral over R*, or shortly *R-integral*, if for some $n \geq 1$ there exist elements $a_0, a_1, \ldots, a_{n-1}$ of R such that the equality

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{1.2}$$

holds, i.e., if x is a root of a monic polynomial of positive degree and coefficients in R.

Note that if R is a field, then the elements integral over R are exactly those which are algebraic over R, i.e., which are roots of non-zero polynomials over R.

One can define R-integrality in another way, which is sometimes better suited for applications. This is the content of the next proposition:

Proposition 1.6. *The following properties of an element x, lying in a field L containing R, are equivalent:*

(i) x is R-integral,

(ii) The ring $R[x]$ generated by R and x is a finitely generated R-module,

(iii) There exists a finitely generated and non-zero R-module $M \subset L$ with $xM \subset M$.

Proof : (i) ⇒ (ii) Observe that the elements $1, x, \ldots, x^{n-1}$, with n as in (1.2), generate $R[x]$.

(ii) ⇒ (iii) The R-module $R[x]$ may serve as M.

(iii) ⇒ (i) Let $z_1, \ldots, z_r$ be generators of M. From $xM \subset M$ we obtain the existence of $b_{ij} \in R$ $(i, j = 1, 2, \ldots, r)$ such that

$$xz_i = \sum_{j=1}^{r} b_{ij} z_j \quad (i = 1, 2, \ldots, r)$$

holds. Since M is non-zero, not all z_i can vanish, and so we have

$$\det[b_{ij} - x\delta^i_j] = 0,$$

where

$$\delta^i_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Expanding this determinant we get an equation of the form (1.2). □

Corollary. *The set of all R-integral elements of a field L (with R being a subring with unit of L) forms a ring.*

Proof : Let $a, b \in L$ be R-integral. Choose finitely generated and non-zero R-modules M, N in L, satisfying $aM \subset M$ and $bN \subset N$. The R-module $MN = \{\sum m_j n_j : \ m_j \in M, n_j \in N\}$ is finitely generated and non-zero, and we have

$$(a \pm b)MN \subset MN, \quad (ab)MN \subset MN,$$

whence $a \pm b$ and ab are R-integral. □

The ring whose existence is asserted in this corollary is called the *integral closure of R in L*. A domain which is equal to its integral closure in its quotient field is called *integrally closed*. We prove now the transitivity of this notion.

Theorem 1.7. *Let R be a domain contained in a field K, and let S be the integral closure of R in K. Then S is integrally closed.*

Proof : Let $x \in K$ be S-integral, i.e., for some $n \geq 1$ and $a_0, \ldots, a_{n-1}$ in S we have $x^n + \sum_{j=0}^{n-1} a_j x^j = 0$. The ring R_1, generated by R and the a_j's, is a finitely generated R-module, as can be seen from the consideration of the chain

$$R \subset R[a_0] \subset R[a_0, a_1] \subset \ldots \subset R[a_0, \ldots, a_{n-1}] = R_1,$$

in which every ring is a finitely generated module over its predecessor. Since x is clearly R_1-integral, Proposition 1.6 shows that $R_1[x]$ is a finitely generated R_1-module, and it follows that it is a finitely generated R-module. As it is obviously non-zero and $xR_1[x] \subset R_1[x]$, Proposition 1.6 implies the R-integrality of x. □

We shall now use the notion of integrality to give a characterization of Dedekind domains:

Theorem 1.8. *A domain R is Dedekind if and only if it satisfies the following three conditions:*

(i) R is Noetherian,

(ii) Every non-zero prime ideal of R is maximal,

(iii) R is integrally closed.

Proof : Necessity. Let first R be a Dedekind domain. Theorem 1.5 shows that the conditions (i) and (ii) are satisfied, and to prove (iii) let x be an R-integral element of the field K of fractions of R. By Proposition 1.6 the ring $R[x]$ is a finitely generated R-module. Let $a_1, \ldots, a_m$ be its generators, and choose $b \neq 0$ in R so that $ba_i \in R$ holds for $i = 1, 2, \ldots, m$. Then $bR[x] \subset R$, showing that $R[x]$ is a fractional ideal. Since it is a ring, we get $R[x]R[x] = R[x]$ and

$$R[x] = RR[x] = R[x]R[x]^{-1}R[x] = R[x]R[x]R[x]^{-1} = R[x]R[x]^{-1} = R,$$

and thus $x \in R$. This shows that R is integrally closed.

Sufficiency. For the proof of this part of the theorem we need three lemmas.

Lemma 1.9. *If R is a Noetherian domain and I is an ideal in R, distinct from $\{0\}$ and R, then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R such that*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset I \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r.$$

Proof : Let I be the maximal element of the set of all those ideals of R which do not have the asserted property. This ideal cannot be prime, since in that case we may take $r = 1$, $\mathfrak{p}_1 = I$. Hence there exist elements $a, b \notin I$ with $ab \in I$. Put $A = I + aR$ and $B = I + bR$. Then $AB \subset I \subset A \cap B$. The ideals A, B are non-zero and not equal to R, since e.g. $A = R$ would imply the equality $B = I$. Hence A and B have the property formulated in the lemma, and this implies that I has it as well. This contradiction proves the lemma. □

Lemma 1.10. *If a domain R satisfies the conditions (i), (ii) and (iii) of the theorem, then every non-zero prime ideal of R is invertible.*

Proof : Let $\mathfrak{p}$ be a non-zero prime ideal in R, and choose a non-zero element $a \in \mathfrak{p}$, so that the principal ideal aR contains a product $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ of the least possible number of non-zero prime ideals. Such choice is possible by Lemma 1.9. If $r = 1$, then $\mathfrak{p} = aR$ is clearly invertible, so we may assume $r \geq 2$. Now one of the ideals $\mathfrak{p}_i$, say $\mathfrak{p}_1$, must be contained in $\mathfrak{p}$, and so by (ii), $\mathfrak{p}_1 = \mathfrak{p}$. The product $\mathfrak{p}_2 \cdots \mathfrak{p}_r$ is not contained in aR, so choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus aR$. Then $b\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset aR$, and $ba^{-1}\mathfrak{p} \subset R$, i.e., $ba^{-1} \in \mathfrak{p}' \setminus R$, showing that $R \subset \mathfrak{p}'$ and $R \neq \mathfrak{p}'$.

The product $\mathfrak{p}\mathfrak{p}'$ is an ideal in R, and, moreover,

$$\mathfrak{p} = R\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}' \subset R.$$

We have to prove $\mathfrak{p}\mathfrak{p}' = R$. Assume this to be false. Then $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$, and consequently for $n = 1, 2, \ldots$ the equality $\mathfrak{p}(\mathfrak{p}')^n = \mathfrak{p}$ holds. Hence for every

non-zero $x \in \mathfrak{p}$ and $y \in \mathfrak{p}' \setminus R$ we have $xy^n \in \mathfrak{p} \subset R$ for all n. This in turn implies $xR[y] \subset R$, thus $xR[y]$ is an ideal of R. By (i) it has a finite set of generators, say $a_1, \ldots, a_m$, and it follows that the R-module $R[y]$ has $a_1x^{-1}, \ldots, a_mx^{-1}$ for generators. Proposition 1.6. shows that y is R-integral, and (iii) implies $y \in R$, contrary to the choice of y. □

Lemma 1.11. *If a domain R satisfies the conditions (i), (ii) and (iii) of the theorem, then every non-zero ideal in R, except R itself, is either a prime ideal, or a product of prime ideals.*

Proof : Let $I \neq R$ be a non-zero ideal in R which is not a product of prime ideals. Lemma 1.9 shows that I contains a product $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ of non-zero prime ideals, and we may assume that I is selected so that r is minimal. If $r = 1$, then (ii) shows that I is a prime ideal, so assume $r \geq 2$. Let $\mathfrak{p}$ be a prime ideal containing I. Then $\mathfrak{p} = \mathfrak{p}_1$, say, and

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = R,$$

whence $\mathfrak{p}^{-1}I$ is an ideal in R. By the choice of I we have $\mathfrak{p}^{-1}I = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with some prime ideals $\mathfrak{q}_i$, and finally $I = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_s$, contradiction. □

Now we may prove our theorem. Let I be a non-zero fractional ideal of R, and let $a \neq 0$ in R be such that $aI \subset R$. Since aI is an ideal of R, we may apply Lemma 1.11 to get $aI = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with suitable prime ideals $\mathfrak{p}_i$, and thus

$$I = a^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r = (a^{-1}R)\mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Lemma 1.10 shows now that I is a product of invertible ideals, and so it must be invertible himself. □

Corollary. *In a Dedekind domain every proper non-zero ideal is either prime or can be represented as a product of prime ideals.*

Proof : Apply the last theorem and Lemma 1.11. □

It turns out that this representation is unique. This is the main property of Dedekind domains.

Theorem 1.12. *If R is a Dedekind domain, then every proper non-zero ideal I of R can be represented uniquely in the form*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

where $\mathfrak{p}_i$ are prime ideals, if products differing in order will not be regarded as distinct.

Proof : Only the uniqueness remains to be proved. Let $I \neq \{0\}$ be a proper ideal of R with two different representations as a product of prime ideals, say

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \quad (r \leq s)$$

We may assume that I is chosen so that r is minimal possible. Now $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1$, hence one of the $\mathfrak{q}_i$'s, say $\mathfrak{q}_1$, is contained in $\mathfrak{p}_1$. By Theorem 1.5 $\mathfrak{q}_1 = \mathfrak{p}_1$, and by Lemma 1.10 we obtain

$$\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1} I = \mathfrak{q}_2\mathfrak{q}_3 \cdots \mathfrak{q}_s.$$

Thus the ideal $\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r$ has two different factorizations into prime ideals, which are different, as the factorizations of I were different. This contradicts the minimality of r. □

Corollary 1. *Every non-zero ideal I of a Dedekind domain R can be uniquely written in the form*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}},$$

where the product is taken over all non-zero prime ideals of R, and the exponents $\alpha_\mathfrak{p}$ are nonnegative integers, of which only finitely many are non-zero. □

Corollary 2. *The group of all fractional ideals of a Dedekind domain R is a free Abelian group generated by the non-zero prime ideals of R.*

Proof : Let I be a fractional ideal of R, and let $aI \subset R$ with a non-zero $a \in R$. Then aI is an ideal of R, hence $I = (aR)^{-1}(aI)$ is a product of powers of prime ideals with integral, not necessarily positive, exponents. Hence the prime ideals generate the group of all fractional ideals, and the last theorem shows that they do it freely. □

Corollary 3. *A non-zero ideal in a Dedekind domain is contained only in finitely many distinct ideals.* □

Now we regain for the ideals of a Dedekind domain many results of elementary number theory connected with the notion of divisibility.

We shall say that a fractional ideal B *divides* A (and write $B|A$) if, with a suitable ideal C of R, one has $A = BC$. The *greatest common divisor* of two ideals A, B is an ideal which divides both A and B, and is divisible by every other ideal having this property. The existence and uniqueness of the greatest common divisor results from Corollary 1 to the last theorem. It should only be noted that if $A = \prod_\mathfrak{p} \mathfrak{p}^{\alpha_\mathfrak{p}}$ and $B = \prod_\mathfrak{p} \mathfrak{p}^{\beta_\mathfrak{p}}$, then B divides A if and only if for all $\mathfrak{p}$ one has $\beta_\mathfrak{p} \leq \alpha_\mathfrak{p}$. This implies that the greatest common divisor of A and B equals $\prod_\mathfrak{p} \mathfrak{p}^{\gamma_\mathfrak{p}}$ with $\gamma_\mathfrak{p} = \min\{\alpha_\mathfrak{p}, \beta_\mathfrak{p}\}$.

Similarly, the *least common multiple* of two ideals is defined as an ideal divisible by both, and dividing every other ideal with this property. It is easy to see that the least common multiple of $A = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$ and $B = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_{\mathfrak{p}}}$ is the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\delta_{\mathfrak{p}}}$ with $\delta_{\mathfrak{p}} = \max\{\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}\}$.

In accordance with the elementary number theory we shall denote the greatest common divisor of ideals A and B by (A, B), and their least common multiple by $[A, B]$. In the case $(A, B) = R$ one says that the ideals A and B are *relatively prime*. In this case we shall write also $(A, B) = 1$.

The reader may prove himself other properties of (A, B) and $[A, B]$ which are analogous to those known from elementary number theory, e.g. the equality $(A, B)[A, B] = AB$.

We conclude this subsection with establishing certain links between the notion of divisibility and set-theoretical properties:

Proposition 1.13. *Let R be a Dedekind domain.*

(i) If A, B are fractional ideals, then the inclusion $A \subset B$ holds if and only if $B|A$,

(ii) If A, B are relatively prime ideals in R, then $AB = A \cap B$,

(iii) If A and B are ideals in R, then $(A, B) = A + B$.

Proof : The implication $B|A \Rightarrow A \subset B$ in (i) is trivial. If $A \subset B$, then $AB^{-1} \subset BB^{-1} = R$, hence $C = AB^{-1}$ is an ideal of R, satisfying $BC = A$.

If A and B are relatively prime ideals of R, then by (i) both A and B divide $A \cap B$, and so $AB|A \cap B$, whence $A \cap B \subset AB$. The converse inclusion being trivial, (ii) follows.

Finally, to obtain (iii) note that in view of (i) $A + B$ divides (A, B), and, on the other hand, $A + B$ is the minimal ideal containing A and B, hence it has to be divisible by (A, B), and it remains to apply (i). □

3. This subsection is devoted to linear congruences modulo an ideal in a Dedekind domain R. Imitating once again the theory of rational integers we shall write $a \equiv b \pmod{I}$ to mean $a - b \in I$, where I is an ideal of R. The following proposition solves the problem of solubility of a linear congruence in any domain, not necessarily Dedekind:

Proposition 1.14. *If R is a domain, I is an ideal in R and $a, b \in R$, then the congruence $ax \equiv b \pmod{I}$ has a solution $x \in R$ if and only if the element b lies in the ideal $I + aR$.*

Proof : If the congruence $ax \equiv b \pmod{I}$ has a solution x, then for a suitable $y \in I$ we have $b = y + ax \in I + aR$, proving the necessity of the condition stated. To prove its sufficiency, observe that $b \in I + aR$ implies $b = ax' + y$ for certain $x' \in R$ and $y \in I$, i.e., x' is a solution of our congruence. □

Corollary 1. *If $\mathfrak{p}$ is a prime ideal in a Dedekind domain R, and $a \in R \setminus \mathfrak{p}$, then for every $b \in R$ and natural n the congruence $ax \equiv b \pmod{\mathfrak{p}^n}$ is solvable in R.*

Proof : It suffices to observe that $\mathfrak{p}^n + aR = R$. □

Corollary 2. *If $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are distinct prime ideals in a Dedekind domain R, then for any given $a_1, \ldots, a_m$ in R and every natural n there exists a common solution of the congruences $x \equiv a_i \pmod{\mathfrak{p}_i^n}$ $(i = 1, 2, \ldots, m)$.*

Proof : For $i = 1, 2, \ldots, m$ choose b_i in $(\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_m)^n \setminus \mathfrak{p}_i$, and let x_i be a solution of the congruence $b_i x_i \equiv a_i \pmod{\mathfrak{p}_i^n}$. The element $x = \sum_{i=1}^m b_i x_i$ has the desired property. □

Corollary 3. (Chinese remainder theorem) *If $I_1, \ldots, I_m$ are pairwise relatively prime ideals in a Dedekind domain R and $a_1, \ldots, a_m \in R$ are given, then there exists a common solution of the congruences $x \equiv a_i \pmod{I_i}$ $(i = 1, 2, \ldots, m)$.*

Proof : Observe that if $I = \prod \mathfrak{p}^{\alpha_\mathfrak{p}}$, then every congruence of the form

$$x \equiv a \pmod{I}$$

is equivalent to the system of congruences $x \equiv a \pmod{\mathfrak{p}^{\alpha_\mathfrak{p}}}$, and apply Corollary 2 with $n = \max_{\mathfrak{p}|I}\{\alpha_p\}$. □

Corollary 4. *Let I, J be relatively prime ideals in a Dedekind domain R. Then one can find an element $x \in I$, which satisfies $(xR, J) = 1$, $(xI^{-1}, I) = 1$, and, moreover, for every ideal I_1 relatively prime to I there exists $y \in I$ with $(yR, I_1) = 1$, $(yI^{-1}, I) = 1$ and $xR + yR = I$.*

Proof : Write $I = \prod_{i=1}^m \mathfrak{p}_i^{\alpha_i}$, and let $x_i \in \mathfrak{p}_i^{\alpha_i} \setminus \mathfrak{p}_i^{\alpha_i+1}$ for $i = 1, 2, \ldots, m$. By Corollary 3 the system

$$\begin{aligned} x &\equiv x_i \pmod{\mathfrak{p}_i^{\alpha_i+1}} \quad (i = 1, 2, \ldots, m), \\ x &\equiv 1 \pmod{J} \end{aligned}$$

has a solution $x \in R$. We may write $xR = II_2$ with an ideal I_2, satisfying $(I_2, IJ) = 1$. Applying once more Corollary 3 we obtain the existence of $y \in R$, satisfying the system

$$\begin{aligned} y &\equiv x_i \pmod{\mathfrak{p}_i^{\alpha_i+1}} \quad (i = 1, 2, \ldots, m), \\ y &\equiv 1 \pmod{I_1 I_2}. \end{aligned}$$

Finally we see that $yR = II_3$ holds with a suitable I_3, satisfying $(I_3, I_2) = (I_3, I_1) = 1$, which is equivalent to our final assertion. □

Corollary 5. *Every ideal in a Dedekind domain R is generated as an R-module by at most two elements.*

Proof : This follows immediately from Corollary 4. □

Corollary 6. *If I and J are ideals in a Dedekind domain R, then there exists an ideal A such that $(A, IJ) = 1$ and the product AI is principal.*

Proof : Write $I = \prod_{\mathfrak{p}} \mathfrak{p}_i^{\alpha_\mathfrak{p}}$, $J = \prod_{\mathfrak{p}} \mathfrak{p}_i^{\beta_\mathfrak{p}}$, and let P be the set of prime ideals dividing IJ. For every $\mathfrak{p} \in P$ choose $x_\mathfrak{p} \in \mathfrak{p}^{\alpha_\mathfrak{p}} \setminus \mathfrak{p}^{\alpha_\mathfrak{p}+1}$. Corollary 3 implies the existence of $a \in R$ satisfying $a \equiv x_\mathfrak{p} \pmod{\mathfrak{p}^{\alpha_p+1}}$ for $\mathfrak{p} \in P$, and for such a we have

$$aR = \prod_p \mathfrak{p}^{\alpha_\mathfrak{p}} \cdot A = IA$$

with some A relatively prime to the product IJ. □

The next theorem reduces the determination of the structure of the factor ring R/I to the case when I is a power of a prime ideal:

Theorem 1.15. *If I is a non-zero ideal in a Dedekind domain R, and*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}}$$

is its factorization into prime ideal powers, then the factor ring R/I is isomorphic to the direct sum

$$\bigoplus_{\mathfrak{p}} R/\mathfrak{p}^{\alpha_p},$$

and the group of invertible elements of R/I is isomorphic with the product of the groups of invertible elements of the rings $R/\mathfrak{p}^{\alpha_p}$.

Proof : Consider the homomorphism $f : R \longrightarrow \bigoplus_{\mathfrak{p}} R/\mathfrak{p}^{\alpha_p}$ given by

$$f(x) = [x \bmod \mathfrak{p}^{\alpha_\mathfrak{p}}]_\mathfrak{p}.$$

Corollary 3 shows that f is surjective, and if x lies in its kernel, Ker f, then $x \in \mathfrak{p}^{\alpha_\mathfrak{p}}$ for all $\mathfrak{p}$, and so $x \in I$, whence Ker f is contained in I. Since the inclusion $I \subset$ Ker f is trivial, we get Ker $f = I$. The last assertion follows immediately. □

4. In this subsection R will be a Dedekind domain having the following *finite norm property* ((FN)-property):

For every non-zero ideal I of R the factor ring R/I is finite.

The number of elements in R/I will be called the *absolute norm* of I, or *norm*, for short, and will be denoted by $N(I)$. Observe that for every I the

ideal $N(I)R$ is divisible by I, since the canonical image of $N(I)e$ (where e is the unit element of R) in R/I is zero. Moreover the norm of a prime ideal is a prime power, since, in this case, by Theorem 1.5, R/I is a finite field. The main properties of the norm are given in the following theorem:

Theorem 1.16. *(i) For non-zero ideals I, J we have $N(IJ) = N(I)N(J)$.*

(ii) For any given positive T the number of ideals I of R, satisfying $N(I) \leq T$ is finite.

Proof : (i) We need a lemma:

Lemma 1.17. *If $\mathfrak{p}$ is a non-zero prime ideal in a Dedekind domain R and n is an arbitrary natural number, then the factor rings $R/\mathfrak{p}$ and $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ have isomorphic additive groups.*

Proof : Choose $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$, and consider the mapping $g : x \mapsto ax$ of the additive group R^+ of R into the additive group of $\mathfrak{p}^n$. Since $g(\mathfrak{p}) \subset \mathfrak{p}^{n+1}$, g induces a homomorphism $\overline{g}$ of the additive group of $R/\mathfrak{p}$ into the additive group of $\mathfrak{p}^n/\mathfrak{p}^{n+1}$. Observe that if $\overline{x}$ lies in the kernel of $\overline{g}$ and x is any representative of $\overline{x}$ in R, then $ax \in \mathfrak{p}^{n+1}$. This implies $x \in \mathfrak{p}$, i.e., $\overline{x} = 0$, and we see that $\overline{g}$ is an injection.

To prove that it is also surjective, take any $\overline{y} \in \mathfrak{p}^n/\mathfrak{p}^{n+1}$, and let y be a representative of $\overline{y}$. Since $(aR, \mathfrak{p}^{n+1}) = \mathfrak{p}^n$, Propositions 1.13 (iii) and 1.14 imply the existence of $\xi \in R$ with $a\xi \equiv y \pmod{\mathfrak{p}^{n+1}}$, and for the element $\overline{\xi}$ of $R/\mathfrak{p}$ containing ξ we clearly have $\overline{g}(\overline{\xi}) = \overline{y}$. Hence $\overline{g}$ is an isomorphism. □

This lemma implies that for every prime ideal $\mathfrak{p}$ the factor ring $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ has $N(\mathfrak{p})$ elements, and since $\#(R/\mathfrak{p}^{n+1})/\#(R/\mathfrak{p}^n) = \#(\mathfrak{p}^n/\mathfrak{p}^{n+1})$, we get $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$ for all n, so it remains to apply Theorem 1.15.

(ii) Since R is infinite, consider a set of more than $1+T$ distinct elements of R, say $a_1, \ldots, a_m$. For every ideal I with $N(I) \leq T$ there exist $i \neq j$ such that a_i and a_j are congruent mod I. The set of differences $a_i - a_j$ being finite, our assertion follows now from Corollary 3 to Theorem 1.12. □

This theorem shows that the norm is a homomorphism of the semigroup of all non-zero ideals of R into the multiplicative semigroup of natural numbers. Corollary 2 to Theorem 1.12 enables us to extend this homomorphism to the group of all fractional ideals of R, the value group being the multiplicative group of positive rationals. This extended homomorphism we shall again denote by $N(I)$, and call it the *norm*.

We shall now prove two results generalizing the theorems of Fermat and Euler in the elementary theory of numbers.

Theorem 1.18. *If $\mathfrak{p}$ is a non-zero prime ideal of R, then for all $x \in R$ one has*

$$x^{N(\mathfrak{p})} \equiv x \pmod{\mathfrak{p}}.$$

Moreover, $N(\mathfrak{p})$ is the least rational integer $n > 1$ such that for all $x \in R$ the congruence $x^n \equiv x \pmod{\mathfrak{p}}$ holds true.

Proof : It suffices to consider the case $x \notin \mathfrak{p}$. Since $R/\mathfrak{p}$ is a field with $N(\mathfrak{p})$ elements, and its multiplicative group is of order $N(\mathfrak{p}) - 1$, Lagrange's theorem implies $x^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$. This proves the first part. To prove the second it suffices to observe that the multiplicative group of any finite field is cyclic, and so for any representative $x \in R$ of its generator the powers $1, x, x^2, \ldots, x^{N(\mathfrak{p})-2}$ are distinct mod $\mathfrak{p}$. □

The number of invertible elements of the factor-ring R/I will be denoted by $\Phi(I)$.

Theorem 1.19. *One has*

$$\Phi(I) = N(I) \prod_{\mathfrak{p}|I} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

where the product is extended over all prime ideals $\mathfrak{p}$ dividing I. Moreover, if $x \in R$ and $(xR, I) = 1$, then

$$x^{\Phi(I)} \equiv 1 \pmod{I}.$$

Proof : In view of Theorem 1.15 and Theorem 1.16 (i) it suffices to prove the first assertion in the case when $I = \mathfrak{p}^n$ is a power of a prime ideal. In this case it is sufficient to observe that

$$\Phi(\mathfrak{p}^n) = N(\mathfrak{p}^n) - N(\mathfrak{p}^{n-1}) = N(\mathfrak{p})^n \left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

The second assertion is a consequence of Lagrange's theorem. □

5. We shall now investigate the behaviour od Dedekind domains under the operation of integral closure. The main result concerning this problem is contained in the following theorem:

Theorem 1.20. *Let R be a Dedekind domain with field of quotients K. Let L/K be a separable extension of K with $n = [L : K]$, and denote by S the integral closure of R in L. Then S is again a Dedekind domain. Moreover, if R satisfies the finite norm property, then S does so as well.*

Proof : We shall check the conditions (i), (ii) and (iii) of Theorem 1.8. Since the extension L/K is separable and finite, it can be generated over K by a

single element, which may be taken from S. In fact, if a generates L/K and is a root of the polynomial

$$A_n X^n + A_{n-1} X^{n-1} + \cdots + A_0 \quad (A_n \neq 0)$$

with coefficients $A_i \in R$, then the element $A_n a$ is a root of

$$X^n + A_{n-1} X^{n-1} + A_{n-2} A_n X^{n-2} + \cdots + A_0 A_n^{n-1},$$

and so it is integral over R, i.e., lies in S.

Consider a fixed algebraic closure Ω of K, and let $L_0, L_1, \ldots, L_{n-1}$ $(n = [L : K])$ be the embeddings of L into Ω. For any $x \in L$ denote by $x^{(i)}$ its image in L_i. We need a lemma which will also be used in the next chapter:

Lemma 1.21. *Let ϑ be an element of S generating the extension L/K. If $D = \det[(\vartheta^{(i)})^k]_{i,k=0,\ldots,n-1}$, then D^2 is a non-zero element of R and $S \subset cR[\vartheta]$ holds with $c = D^{-2}$.*

Proof : The non-vanishing of D follows from the observation that it is a Vandermonde determinant. Now let α be an arbitrary element of S. With suitable $a_0, a_1, \ldots, a_{n-1} \in K$ we can write

$$\alpha = \sum_{k=0}^{n-1} a_k \vartheta^k.$$

It follows that for $i = 1, 2, \ldots, n$ we have

$$\alpha^{(i)} = \sum_{k=0}^{n-1} a_k (\vartheta^{(i)})^k,$$

and thus Cramer's formula shows that $a_k = A_k/D$, where A_k is a determinant whose elements are integral over R. Observe that D^2 is invariant under automorphisms from the Galois group of the least normal extension of K containing L, whence $D^2 \in K$. But D^2 is integral over R, thus lies in R.

Since $a_k = A_k D/D^2$ $(k = 0, 1, \ldots, n-1)$ and $a_k \in K$, $D^2 \in R$, hence $A_k D \in K$, but $A_k D$ is integral over K, hence $A_k D \in R$, and we obtain $D^2 \alpha \in R[\vartheta]$. The inclusion $S \subset cR[\vartheta]$ follows now with $c = D^{-2}$. □

The mapping $f : R^n \longrightarrow cR[\vartheta]$ given by

$$f : (x_0, \ldots, x_{n-1}) \mapsto c \sum_{i=0}^{n-1} x_i \vartheta^i$$

is a surjective homomorphism of R-modules, and by Proposition 1.2 we see that $cR[\vartheta]$ is a Noetherian R-module, and, since $S \subset cR[\vartheta]$, S must be also Noetherian. But every ideal of S is an R-module, and so S is a Noetherian

ring. This proves that condition (i) of Theorem 1.8 is satisfied by S. Since the quotient field of S equals L, Theorem 1.7 implies that condition (iii) is also satisfied by S, and it remains to show that every non-zero prime ideal of S is maximal. For this purpose we prove a lemma:

Lemma 1.22. *Under the assumptions of Theorem* 1.20, *if* $\mathfrak{P}$ *is a prime ideal of* S, *then* $\mathfrak{P} \cap R$ *is also a prime ideal of* R, *and the ring* $R/(\mathfrak{P} \cap R)$ *is a subring of* $S/\mathfrak{P}$. *Moreover, if for prime ideals* $\mathfrak{P}_1$, $\mathfrak{P}_2$ *of* S *we have*

$$\mathfrak{P}_1 \subset \mathfrak{P}_2 \quad \text{and} \quad \mathfrak{P}_1 \cap R = \mathfrak{P}_2 \cap R,$$

then $\mathfrak{P}_1 = \mathfrak{P}_2$.

Proof : Clearly $I = \mathfrak{P} \cap R$ is an ideal of R. The injection $R \longrightarrow S$ carries I into $\mathfrak{P}$, and so it induces a homomorphism of the factor rings $R/I \longrightarrow S/\mathfrak{P}$, which is clearly again an injection. Since $\mathfrak{P}$ is prime, $S/\mathfrak{P}$ has no zero-divisors, and so R/I has the same property, showing that I is a prime ideal.

Now assume that $\mathfrak{P}_1$, $\mathfrak{P}_2$ are distinct prime ideals of S, satisfying $\mathfrak{P}_1 \cap R = \mathfrak{P}_2 \cap R$ and $\mathfrak{P}_1 \subset \mathfrak{P}_2$. Take any element $x \in \mathfrak{P}_2 \setminus \mathfrak{P}_1$, and let

$$X^m + \sum_{i=0}^{m-1} a_i X^i$$

be its minimal polynomial over R. If all coefficients a_i lie in $\mathfrak{P}_1 \cap R$, then $x^m \in \mathfrak{P}_1$ and $x \in \mathfrak{P}_1$, contrary to the choice of x. Therefore there is a minimal index j such that $a_j \notin \mathfrak{P}_1 \cap R$. Then we have

$$x^j(x^{m-j} + a_{m-1}x^{m-j-1} + \cdots + a_j) \in \mathfrak{P}_1,$$

thus

$$x^{m-j} + a_{m-1}x^{m-j-1} + \cdots + a_{j+1}x + a_j \in \mathfrak{P}_1 \subset \mathfrak{P}_2.$$

But $x^{m-j} + \cdots + a_{j+1}x$ lies in $\mathfrak{P}_2$, implying $a_j \in \mathfrak{P}_2$, hence $a_j \in \mathfrak{P}_2 \cap R = \mathfrak{P}_1 \cap R$, contrary to the choice of j. This contradiction proves the lemma. □

Now it is easy to verify the condition (ii). If $\mathfrak{P}_1$ is a non-zero, non-maximal prime ideal of S, then it is contained in a maximal (and *a fortiori* prime) ideal $\mathfrak{P}_2$. The lemma just proved shows that the prime ideals $\mathfrak{P}_1 \cap R$ and $\mathfrak{P}_2 \cap R$ of R are distinct, but clearly the first of them is contained in the second, which is possible only if $\mathfrak{P}_1 \cap R = \{0\}$. However in this case we have $\mathfrak{P}_1 \cap R = \{0\} \cap R$, and the lemma gives $\mathfrak{P}_1 = \{0\}$, contradiction.

Assume finally that R satisfies the finite norm property. Lemma 1.22 shows that for an arbitrary non-zero prime ideal $\mathfrak{P}$ of S the field $k_1 = S/\mathfrak{P}$ is an extension of the finite field $k = R/\mathfrak{p}$, with $\mathfrak{p} = \mathfrak{P} \cap R$. Since every element of S is a root of a monic polynomial over R of degree not exceeding n, it follows that every element of k_1 is algebraic over k of degree $\leq n$. Therefore the extension $[k_1 : k]$ is finite, hence k_1 is a finite field. This shows that the

norm of every non-zero prime ideal of S is finite, and it remains to apply Theorem 1.15 to obtain the finite norm property for S. □

Corollary. *If K is a finite extension of the field of rational numbers, then the integral closure of $\mathbb{Z}$ in K is a Dedekind domain with the (FN)-property.*

Proof : This follows from the theorem and the observation that every finite extension of $\mathbb{Q}$ is separable, and $\mathbb{Z}$ is a Dedekind domain with the (FN)-property. □

1.2. Valuations and Exponents

1. In this section we present the definitions and properties of valuations which will be needed in the sequel.

Let K be any field. A homomorphism v of its multiplicative group K^* into the group of positive reals is called a *valuation*, if it satisfies the condition

$$v(x+y) \leq v(x) + v(y)$$

for all $x, y \in K^*$. By putting $v(0) = 0$ one extends any valuation to the whole field K.

Since from $v(1) = v(-1)^2$ follows $v(-1) = 1$, we get for all $x \in K$ the equality $v(-x) = v(x)$, and this implies that every valuation v induces in K a metric $d(x,y) = v(x-y)$ under which the additive and multiplicative groups of K become topological groups. In fact, continuity of addition is a consequence of $v(-x) = v(x)$, and to check the continuity of multiplication choose $a, b \in K^*$ and a positive ϵ. If $M = \max\{v(a), v(b)\}$ and $\delta \leq \min\{1, \epsilon(1+2M)^{-1}\}$, then the equalities $v(x-a) < \delta$ and $v(y-b) < \delta$ easily imply $v(xy-ab) < \epsilon$. Finally, the continuity of the inverse in K^* follows from $v(x^{-1}) = v(x)^{-1}$. Hence K becomes a topological field. Note that it is not necessarily complete or locally compact, as is shown by the example of the field $\mathbb{Q}$ of rational numbers under the valuation $v(x) = |x|$.

The valuation defined by $v(x) = 1$ for all $x \in K^*$ is called the *trivial valuation*. It induces the discrete topology.

Two valuations are said to be *equivalent* if they define the same topology. The connection between such valuations is given in the following proposition:

Proposition 1.23. *If v and w are equivalent valuations of a field K, then with a suitable positive a one has the equality $w(x) = v(x)^a$ for all $x \in K$.*

Proof : If $v(x) = 1$ for all $x \neq 0$, then v induces the discrete topology, and so $w(x) = 1$ must hold for all $x \neq 0$, since the existence of an element x with $0 < w(x) \neq 1$ would imply either $\lim x^n = 0$ or $\lim x^{-n} = 0$. Assume thus that v is non-trivial, choose x_0 with $v(x_0) > 1$, and put

$$a = \frac{\log w(x_0)}{\log v(x_0)}.$$

Note that the sets $\{x \in K : v(x) > 1\}$ and $\{x \in K : w(x) > 1\}$ coincide, since they are formed by those elements $x \in K$ for which x^{-n} tends to zero in the induced topology. Now fix a non-zero $x \in K$, put

$$b_1 = \frac{\log w(x)}{\log w(x_0)} \quad \text{and} \quad b_2 = \frac{\log v(x)}{\log v(x_0)},$$

and let $r = m/n$ be any rational number larger than b_1. Then $w(x_0^m) > w(x^n)$, whence $w(x_0^m x^{-n}) > 1$, and thus $v(x_0^m x^{-n}) > 1$, i.e., $v(x_0^m) > v(x^n)$ and $r \geq b_2$. Thus $b_1 \geq b_2$, and by symmetry we get $b_2 \geq b_1$, thus $b_1 = b_2$, showing that the ratio $\log w(x)/\log v(x)$ does not depend on x, and our assertion follows. □

If a valuation v satisfies the condition

$$v(x + y) \leq \max\{v(x), v(y)\} \tag{1.3}$$

for all $x, y \in K$, then it is called a *non-Archimedean valuation*. Otherwise it is called an *Archimedean valuation*.

Proposition 1.24. *If v is a non-Archimedean valuation and $v(a) \neq v(b)$, then*

$$v(a + b) = \max\{v(a), v(b)\}.$$

Proof : Assume $v(a) < v(b)$. Then $v(a+b) \leq v(b)$, but on the other hand we have

$$v(b) = v((a + b) - a) \leq \max\{v(a + b), v(a)\},$$

and since the inequality $v(b) \leq v(a)$ is ruled out, we must have $v(b) \leq v(a+b)$. □

The traditional formulation of the Archimedean axiom runs as follows:

(A) *If a and b are non-zero elements of K, then with a suitable positive integer n we have $v(na) > v(b)$.*

(Here and below we identify the natural number n with the sum of n copies of the unit element of the field).

The non-Archimedean valuations are exactly those which disobey the axiom (A). This is contained in the next proposition.

Proposition 1.25. *If v is a valuation of a field K, then the following properties are equivalent:*

(i) *v is non-Archimedean,*

(ii) *For every positive integer* n *one has* $v(n) \leq 1$,

(iii) *There exists a number* $B > 0$ *such that for every positive* n *one has* $v(n) \leq B$,

(iv) v *does not satisfy* (A).

Proof : (i) $\Rightarrow$ (ii). Inequality (1.3) implies $v(n) \leq v(1) = 1$.

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (iv). For every positive integer a we have $v(na) = v(n)v(a) \leq Bv(a)$, whence if we choose b so that $v(b)$ exceeds $Bv(a)$, then (A) will fail. Such a choice is always possible for non-trivial v, since $v(x) > 1$ implies $\lim_{m\to\infty} v(x^m) = \infty$. If, however, v is trivial, then (A) clearly does not hold.

(iv) $\Rightarrow$ (ii). Choose a, b so that for all positive integers n we have $v(na) \leq v(b)$. Then $v(n) \leq v(ba^{-1})$. If, for some n_0, $v(n_0) > 1$ holds, then with a suitable k we have $v(n_0^k) > v(ba^{-1})$, a contradiction.

(ii) $\Rightarrow$ (i). Let a, b be elements of K. If at least one of them is zero, then the assertion becomes obvious, so assume that $b \neq 0$. Clearly we have

$$v((a+b)^n) \leq \sum_{k=0}^{n} v\left(\binom{n}{k} a^k b^{n-k}\right) \leq \sum_{k=0}^{n} v(a)^k v(b)^{n-k}.$$

Now, if $k = 0, 1, \ldots, n$ and $v(a) \leq v(b)$, then we get $v(a)^k v(b)^{n-k} \leq v(b)^n$, and if $v(b) \leq v(a)$, then $v(a)^k v(b)^{n-k} \leq v(a)^n$, thus in any case we arrive at

$$v((a+b)^n) \leq (n+1)\max\{v(a)^n, v(b)^n\},$$

hence

$$v(a+b) \leq (n+1)^{1/n}\max\{v(a), v(b)\},$$

and (1.3) follows. □

Corollary. *If the field* K *has a non-zero characteristic, then all its valuations are non-Archimedean.*

Proof : The set $\{1, 1+1, 1+1+1, \ldots\}$ being finite, the condition (iii) is obviously satisfied. □

2. A valuation v is called *discrete* if the set of values of $\log v$ is discrete. Such valuations are closely connected with the *exponents* of K, i.e., surjective homomorphisms $\nu : K^* \to \mathbb{Z}$ which satisfy the condition

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\} \tag{1.4}$$

for all non-zero $a, b \in K$.

If $0 < c < 1$ and ν is an exponent of K, then $v(x) = c^{\nu(x)}$ is a discrete valuation of K, non-Archimedean by (1.4). Conversely, one can easily see

that every non-trivial discrete non-Archimedean valuation can be obtained in such way from a suitable exponent.

There is a standard way of constructing exponents in the field K of quotients of a Dedekind domain R. Take any non-zero prime ideal P of R, and let x be a non-zero element of K. We may write $xR = P^{\nu(x)}I$ where $\nu(x) \in \mathbb{Z}$ and I is a fractional ideal whose decomposition into prime ideals does not contain P. In this way one defines a function $\nu(x)$ which is an exponent of K. One may define a valuation using that exponent in many ways, depending on the choice of c in the formula $v(x) = c^{\nu(x)}$. However, in the case when R satisfies the finite norm condition it is convenient to make a particular choice of c, namely $c = N(P)^{-1}$. In this case we speak of a *normalized valuation* corresponding to P, and denote it by v_P.

Note that different prime ideals P_1, P_2 induce non-equivalent valuations. In fact, if $x_n \in P_1^n \setminus P_2$, then x_n tends to zero in the topology induced by v_{P_1}, but not by v_{P_2}.

The topology induced in K by the valuation v_P is called the *P-adic topology*. In the ring of rational integers every prime ideal is generated by a rational prime p, and the resulting topology is called the *p-adic topology*.

For an arbitrary exponent ν of K put

$$R_\nu = \{x \in K : \ \nu(x) \geq 0\} \quad \text{and} \quad P_\nu = \{x \in K : \ \nu(x) > 0\}.$$

Theorem 1.26. *The set R_ν is a principal ideal domain (hence Dedekind) and P_ν is its unique non-zero prime ideal. It is generated by every element $\pi \in K$, satisfying $\nu(\pi) = 1$, and for $k = 1, 2, \ldots$ one has*

$$P_\nu^k = \pi^k R_\nu = \{a \in K : \ \nu(a) \geq k\}.$$

Proof : It follows from the definition of the exponent that R_ν is a ring, and P_ν is an ideal in R_ν. If a is a non-zero element of $R_\nu \setminus P_\nu$, then $\nu(a) = 0$, thus $\nu(a^{-1}) = 0$ and $a^{-1} \in R_\nu$, i.e., a is invertible. This shows that P_ν consists of all non-invertible elements of R_ν, and so it is the only maximal ideal of R_ν. To show that P_ν is principal consider any element π with $\nu(\pi) = 1$. Obviously $\pi R_\nu \subset P_\nu$, and for every $a \in P_\nu$ with, say, $\nu(a) = m$ we have $a\pi^{-m} \in R_\nu$. Thus

$$a = \pi^m(a\pi^{-m}) \in \pi^m R_\nu \subset \pi R_\nu,$$

whence $P_\nu \subset \pi R_\nu$, and finally $P_\nu = \pi R_\nu$. This implies immediately the last assertion of the theorem, hence it remains to show that every ideal in R_ν is principal. Let I be a non-zero proper ideal of R_ν. Since P_ν is the unique maximal ideal, we have $I \subset P_\nu$. As the intersection of all powers of P_ν equals the zero ideal we may choose a positive integer N such that $I \subset P_\nu^N$ and $I \not\subset P_\nu^{N+1}$, therefore there exists $a \in I$ with $\nu(a) = N$. Then $a = \pi^N b$ with $b \in R_\nu$ and $\nu(b) = 0$, and this shows that b is invertible in R_ν. Thus the ideals aR_ν and $\pi^N R_\nu$ coincide, but

$$P_\nu^N = \pi^N R_\nu = aR_\nu \subset I,$$

and we obtain $I = P_\nu^N$. It follows that I is principal. □

The ring R_ν is called the *exponent ring* of ν, and if v is a valuation induced by ν, then R_ν is also called the *valuation ring* of v. Similarly, the ideal P_ν is called the *ideal of the exponent* ν (or the *valuation ideal* of v).

We shall now consider more closely the case when ν is the exponent induced by a prime ideal of a Dedekind domain.

Proposition 1.27. *Let R be a Dedekind domain with field of quotients K, let P be a non-zero prime ideal of R, and let ν be the exponent induced by P. Then we have:*

(i) $R_\nu = \{a/b \in K : a \in R, b \in R \setminus P\}$ *and* $P_\nu = \{a/b \in K : a \in P, b \in R \setminus P\}$,

(ii) $P_\nu^m \cap R = P^m$, $(m = 1, 2, \ldots)$,

(iii) $P_\nu^m = P^m R_\nu$, $(m = 1, 2, \ldots)$,

(iv) *The factor-rings R/P^m and R_ν/P_ν^m are isomorphic for $m = 1, 2, \ldots$,*

(v) *The intersection of the rings R_ν, taken over all non-zero prime ideals P of R, equals R.*

Proof : (i) If $a, b \in R$, $b \notin P$, then $\nu(a/b) \geq 0$, hence $a/b \in R_\nu$. If $x \in R_\nu$, then we can write $xR = IJ^{-1}$, where I, J are ideals of R and $P \nmid J$. By Corollary 6 to Proposition 1.14 there is an ideal $A \subset R$ not divisible by P, for which the product AJ is principal. Then $xR = (AI)(AJ)^{-1}$, both ideals AI and AJ are principal, and if $AI = aR$, $AJ = bR$, then $b \notin P$, and with a suitable $c \in R$ we get $x = ac/b$. This establishes the first equality, and to obtain the second it suffices to observe that if π is an element of $P \setminus P^2$, then Theorem 1.26 shows that $P_\nu = \pi R_\nu$.

(ii) This assertion follows from the observation that

$$P^m = \{a \in R : \ \nu(a) \geq m\}.$$

(iii) Theorem 1.26 shows that $P_\nu = \pi R_\nu$ with $\pi \in P \setminus P^2$, thus $P_\nu \subset PR_\nu$. On the other hand, every $x \in PR_\nu$ can be written as $x = a_1 b_1 + \cdots + a_k b_k$ with $a_i \in R$, $\nu(a_i) \geq 1$ and $b_i \in K$, $\nu(b_i) \geq 0$. Hence $\nu(x) \geq \min_i\{\nu(a_i b_i)\} \geq 1$. This implies $x \in P_\nu$, hence $PR_\nu \subset P_\nu$. Thus $PR_\nu = P_\nu$ follows, and the equality $P_\nu^m = P^m R_\nu$ results immediately.

(iv) In view of the embedding $P^m \subset P^m R_\nu = P_\nu^m$ the embedding $R \subset R_\nu$ induces a homomorphism $f : \ R/P^m \longrightarrow R_\nu/P_\nu^m$. We shall now show that f is an isomorphism. Let $\overline{a} \in R/P^m$, $a \in \overline{a}$, and assume that $\overline{a} \in$ Ker f. Since $f(\overline{a})$ is the coset mod P_ν^m determined by a in R_ν, we have $a \in P^m R_\nu \cap R = P^m$ in view of (ii), thus $\overline{a} = 0$. So f is an embedding.

Now let $a \in R_\nu$ and put $r = \nu(a)$. To prove that f is surjective it suffices to find $x \in R$ satisfying $a - x \in P_\nu^m$. If $r \geq m$, then we can take $x = 0$, so

assume $r < m$. By (i) we may write $a = a_1/a_2$ with $a_1 \in R$ and $a_2 \in R \setminus P$. By Corollary 1 to Proposition 1.14, the congruence $a_2 x \equiv a_1 \pmod{P^m}$ has a solution in R, and for this solution we have

$$\nu(a - x) = \nu(a_1 - a_2 x) - \nu(a_2) \geq m,$$

i.e., $a - x \in P_\nu^m$, and $f(x \bmod P^m) = a \bmod P_\nu^m$, proving the surjectivity of f.

(v) The inclusion $R \subset \bigcap R_\nu$ is obvious, and if $a \in K$ is such that for all prime ideals of R the corresponding exponents are non-negative at a, then aR is an ideal of R, whence $a \in R$. □

3. In this subsection we shall prove the *weak approximation theorem* for valuations, due to Artin and Whaples [45], which can be regarded as an abstract version of the Chinese remainder theorem, to which it reduces in the case when all valuations occurring in its statement are induced by prime ideals of a Dedekind domain R with quotient field K, and the elements a_i belong to R.

Theorem 1.28. *Let $v_1, \ldots, v_t$ be non-equivalent and non-trivial valuations of a field K, let $a_1, \ldots, a_t \in K$, and let $\epsilon > 0$ be given. Then there exists $a \in K$ such that for $i = 1, 2, \ldots, t$ one has $v_i(a - a_i) < \epsilon$.*

Proof : We follow the argument of Artin and Whaples:

Lemma 1.29. *Under the assumptions of the theorem there exists $x \in K$ with $v_1(x) > 1$ and $v_i(x) < 1$ for $i = 2, 3 \ldots, t$.*

Proof : First let $t = 2$. Since v_1 and v_2 are inequivalent, there exists a sequence $\{x_n\}$ such that $v_2(x_n)$ tends to zero, whereas $v_1(x_n) \geq \delta$ holds for a certain fixed $\delta > 0$. Select $c \in K$ with $v_1(c) > 1/\delta$. If we take n to be sufficiently large, so that $v_2(x_n) < v_2(c)^{-1}$ holds, then for $a = cx_n$ we get

$$v_2(a) = v_2(c)v_2(x_n) < 1 \quad \text{and} \quad v_1(a) = v_1(c)v_1(x_n) > 1.$$

In the general case we proceed by induction, and assume that $t \geq 3$ and the lemma is true for all systems of $t - 1$ valuations. Choose $a, b \in K$ so that the inequalities

$$\begin{aligned} &v_1(a) > 1, \quad v_j(a) < 1 \quad (j = 2, 3, \ldots, t-1), \\ &v_1(b) > 1, \quad v_t(b) < 1 \end{aligned}$$

are satisfied. If $v_t(a) \leq 1$, then for sufficiently large n the element $x = a^n b$ fulfils our assertion, and if $v_t(a) > 1$, then define $x_n \in K$ (for $n = 1, 2, \ldots$) by $x_n = a^n b(1 + a^n)^{-1}$. For $j = 2, 3, \ldots, t - 1$ we obtain

$$v_j(x_n) = \frac{v_j(a)^n v_j(b)}{v_j(1 + a^n)} \leq \frac{v_j(a)^n v_j(b)}{1 - v_j(a)^n},$$

and for $j = t$ we obtain

$$v_t(x_n) \leq v_t(a)^n v_t(b)(v_t(a)^n - 1)^{-1}.$$

In both cases, for sufficiently large n, the right-hand side of the inequalities is less than 1, since if $v_t(a) > 1$, then

$$\lim_{n\to\infty} \frac{v_t(a)^n}{v_t(a)^n - 1} = 1.$$

Moreover, we have

$$v_1(x_n) \geq v_1(a)^n v_1(b)(1 + v_1(a)^n)^{-1},$$

and we see that for large n the element x_n satisfies our needs. □

Lemma 1.30. *Under the assumptions of the theorem there exists an element $y \in K$ satisfying*

$$v_1(y - 1) < \epsilon \quad \text{and} \quad v_j(y) < \epsilon \quad (j = 2, 3, \ldots, t).$$

Proof : The preceding lemma gives the existence of $a \in K$ with $v_1(a) > 1$ and $v_j(a) < 1$ for $j = 2, 3, \ldots, t$. It suffices now to put $y = a^n(1 + a^n)^{-1}$ with n sufficiently large. □

The theorem follows now easily. Let M be a positive integer exceeding $\max_{i,j} v_i(a_j)$, and choose $x_i \in K$ satisfying

$$v_i(x_i - 1) < \frac{\epsilon}{tM}, \quad v_j(x_i) < \frac{\epsilon}{tM} \quad (j \neq i)$$

for $i = 1, 2, \ldots, t$. The element $a = \sum_{i=1}^{t} a_i x_i$ satisfies our assertion. □

Corollary. *Let $v_1, \ldots, v_t$ be non-equivalent and non-trivial non-Archimedean valuations of a field K. If non-zero $a_1, \ldots, a_t \in K$ are given, then there exists $x \in K$ satisfying $v_j(x) = v_j(a_j)$ for $j = 1, 2, \ldots, t$.*

Proof : Applying Theorem 1.28 with $\epsilon = \min_j v_j(a_j)$ we get an element $x \in K$ with $v_j(x - a_j) < \epsilon$ for $j = 1, 2, \ldots, t$. If for a certain j we had $v_j(x) \neq v_j(a_j)$, then by Proposition 1.24 we would have

$$v_j(x - a_j) = \max\{v_j(x), v_j(a_j)\} \geq v_j(a_j) \geq \epsilon,$$

contradicting the choice of x. □

4. We conclude this section with a description of all valuations of the field $\mathbb{Q}$ of rational numbers. In Chap.3 we shall describe valuations of finite extensions of $\mathbb{Q}$.

Theorem 1.31. *If v is a non-trivial valuation of $\mathbb{Q}$, then either v is equivalent to the ordinary absolute value $|a|$ or it is equivalent to one of the p-adic valuations induced by rational primes.*

Proof : Assume first that v is Archimedean. Let $m, n > 1$ be integers, and write

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

with integers $0 \leq a_i < n$ and non-zero a_r. Then

$$v(m) \leq v(a_0) + \cdots + v(a_r) v(n)^r,$$

and since for all positive rational integers N we have

$$v(N) \leq \sum_{j=1}^{N} v(1) = N,$$

it follows that

$$v(m) \leq n(1 + v(n) + \cdots + v(n)^r) \leq n(r+1) \max\{1, v(n)^r\}.$$

However, $n^r \leq m$ and so $r \leq \log m / \log n$, implying

$$v(m) \leq n \left(1 + \frac{\log m}{\log n}\right) \max\{1, v(n)^{\log m / \log n}\}.$$

Now put $m = M^k$ with a fixed $M > 1$, extract the kth roots of both sides, and let k tend to infinity. In this way we get the inequality

$$v(M) \leq \max\{1, v(n)^{\log M / \log n}\}, \tag{1.5}$$

valid for every pair M, n of integers larger than 1. Since v is Archimedean, we may choose M with $v(M) > 1$, and obtain

$$v(n)^{\log M / \log n} > 1,$$

which proves $v(n) > 1$ for all integers $n > 1$. But this together with (1.5) implies

$$v(M) \leq v(n)^{\log M / \log n} > 1,$$

i.e.

$$\frac{\log v(M)}{\log M} \leq \frac{\log v(n)}{\log n}$$

for all integers $M, n > 1$. Interchanging M and n we finally obtain that the ratio

$$\frac{\log v(n)}{\log n}$$

does not depend on n, i.e., for all integers $n > 1$ we have $v(n) = n^c$ with a certain constant c. This implies $v(x) = |x|^c$ for all rational x, and so v is equivalent to the usual absolute value.

Now let v be non-Archimedean. By Proposition 1.25 we have $v(n) \leq 1$ for all integers n. Let A be the set of all those integers n for which $v(n) < 1$. If $A = \{0\}$, then v is trivial, which case we excluded. Thus A is a non-zero, and since $1 \notin A$ we get from (1.3) that A is a proper non-zero ideal in $\mathbb{Z}$, thus $A = m\mathbb{Z}$ with a suitable positive integer m. Since obviously m is the smallest positive element of A, it must be prime, because a factorization $m = rs$ with $r, s > 1$ would imply $1 > v(m) = v(r)v(s) = 1$, which is impossible. Put $v(m) = a$ and denote by ν the exponent induced by the prime ideal $m\mathbb{Z}$. Then $v(x) = a^{\nu(x)}$, hence v is a p-adic valuation induced by the prime $p = m$. □

Corollary. *If v is a discrete valuation of a field K, then it is non-Archimedean.*

Proof: Assume that v is Archimedean. Corollary to Proposition 1.25 implies that K is of zero characteristic, and thus contains $\mathbb{Q}$. The restriction of v to $\mathbb{Q}$ must be Archimedean, and so by the theorem it must be equivalent to $|x|$, whence non-discrete. □

1.3. Finitely Generated Modules over Dedekind Domains

1. We shall now be concerned with the structure of finitely generated modules over a Dedekind domain R with the field of quotients K. This structure is described by the following result, essentially due to Steinitz [12]:

Theorem 1.32. *Let M be a finitely generated R-module, and let A be its submodule consisting of all torsion elements, i.e., of all elements $x \in M$ which, for some non-zero $r \in R$, satisfy $rx = 0$. Then M can be written as a direct sum*

$$M = R^k \oplus I \oplus A,$$

where k is a non-negative integer, and I is an ideal of R.

For the proof of this theorem we shall need various results concerning projective modules over commutative rings, not necessarily Dedekind.

If R is a commutative ring with unit element 1, then an R-module M is called *projective* if every diagram of the form

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

with exact row and arbitrary R-modules A, B can be embedded in a commutative diagram

$$\begin{array}{ccccc} & & M & & \\ & \swarrow & \downarrow & & \\ A & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

Proposition 1.33. *The direct sum $P = \bigoplus P_a$ of R-modules is projective if and only if every summand P_a is projective.*

Proof : Denote by i_a the canonical injection of P_a into P and by p_a the canonical projection of P onto P_a. Assume now that P is projective, the sequence $A \longrightarrow B \longrightarrow 0$ is exact, and $f : P_a \longrightarrow B$ is a homomorphism. Then $f_1 = f \circ p_a$ is a homomorphism of P into B, hence, by our assumption, there exists a homomorphism $g : P \longrightarrow A$ such that the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow_g & \downarrow_{f_1} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutes. Now it suffices to observe that the mapping $h = g \circ i_a$ makes the diagram

$$\begin{array}{ccccc} & & P_a & & \\ & \swarrow_h & \downarrow_f & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutative, and so P_a is projective.

To prove the second part of the proposition assume that all modules P_a are projective, the sequence $A \longrightarrow B \longrightarrow 0$ is exact, and a homomorphism $f : P \longrightarrow B$ is given. Then $f_a = f \circ i_a$ maps P_a in B, hence with a suitable $g_a : P_a \longrightarrow A$ the diagram

$$\begin{array}{ccccc} & & P_a & & \\ & \swarrow_{g_a} & \downarrow_{f_a} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutes. The projectivity of P follows now from the observation that the map $h = \oplus g_a$ makes the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow_h & \downarrow_f & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutative. □

Corollary. *Every free R-module if projective.*

Proof : As every free R-module is a direct sum of R-modules R, it suffices to establish the projectivity of R. Let $f : R \longrightarrow B$ be a homomorphism, and let the sequence $A \xrightarrow{g} B \longrightarrow 0$ be exact. If $f(1) = b$ and a is any element of A with $g(a) = b$, then the map $h : R \longrightarrow A$ given by $h(x) = xa$ has the required property. □

The properties of an R-module equivalent to its projectivity are established in the following simple proposition:

Proposition 1.34. *The following properties of an R-module M are equivalent:*

(i) *If the sequence* $0 \longrightarrow A \longrightarrow B \longrightarrow M \longrightarrow 0$ *is exact, then* $A \oplus M \sim B$,

(ii) *M is a direct summand of a suitable free R-module,*

(iii) *M is projective.*

Proof : (i) $\Rightarrow$ (ii). The module M is a homomorphical image of a free module F, and so for a suitable N the sequence $0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0$ is exact. By (i) we have $F \sim M \oplus N$.

(ii) $\Rightarrow$ (iii). If $M \oplus N \sim F$ and F is free, then by the Proposition 1.33 and its Corollary we get the projectivity of M.

(iii) $\Rightarrow$ (i). Assume that the sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} M \longrightarrow 0$$

is exact. Condition (iii) implies the existence of $f : M \longrightarrow B$ making the composition $M \xrightarrow{f} B \xrightarrow{p} M$ the identity map. Obviously f is an injection. If $x \in B$, then $f \circ p(x) = y$ lies in Im $f \sim M$. Moreover $p(x - y) = 0$, thus $x - y$ lies in the image of i, and we may write $x = z + y$ with $z \in$ Im i. Finally we see that Im $f \cap$ Im $i = 0$, since for $x \in$ Im $f \cap$ Im $i = 0$ one has $x = f(u)$ with some $u \in A$ and $p(x) = 0$, giving $u = p(f(u)) = 0$. Thus $x = f(0) = 0$. This implies $B \sim$ Im $i \oplus$ Im f, which in turn implies $B \sim A \oplus M$. □

Another characterization of projective modules is provided by the next result:

Proposition 1.35. *An R-module M is projective if and only if there exists a system $(a_t)_{t \in T}$ of elements of M and a family $(f_t)_{t \in T}$ of homomorphisms of M into R such that every element $a \in M$ can be written in the form*

$$a = \sum_{t \in T} f_t(a) a_t, \tag{1.6}$$

where only for finitely many t one has $f_t(a) \neq 0$.

Proof : Assume first that M is projective, and let F be any free R-module whose image by a homomorphism, say f, is M. Proposition 1.34 (i) shows that M is a direct summand of F, and so, with a suitable homomorphism $i : M \longrightarrow F$, we have $f \circ i =$ the identity on M. If $(x_t)_{t\in T}$ is a system of free generators of F, then for every $a \in M$ we have

$$i(a) = \sum_t f_t(a)x_t$$

with some $f_t(a) \in R$. Putting $a_t = f(x_t)$ we get

$$a = \sum_t f_t(a)a_t$$

with only finitely many non-zero summands. Since, obviously, the maps $f_t : M \longrightarrow R$ are homomorphisms we arrive at our assertion.

To prove the converse assume that each $a \in M$ has the form (1.6). Let F be the free R-module with free generators x_t ($t \in T$), and define a homomorphism $f : F \longrightarrow M$ by putting $f(x_t) = a_t$. If now $g : M \longrightarrow F$ is given by

$$g(a) = \sum_t f_t(a)x_t$$

for $a = \sum_t f_t(a)a_t$, then the composition $M \xrightarrow{g} F \xrightarrow{f} M$ equals the identity, showing that M is a direct summand of F, which allows us to conclude, by Proposition 1.34 (ii), that M is projective. □

Our next proposition connects the notion of projectivity with concepts developed in Sect. 1.

Proposition 1.36. *If R is a domain and I is a non-zero ideal in R, then I is projective as an R-module if and only if it is invertible.*

Proof : Let I be an invertible ideal in R, i.e., $II^{-1} = R$. Then, with suitable $a_1, \ldots, a_n \in I$ and $x_1, \ldots, x_n \in I^{-1}$ we have

$$\sum_{i=1}^{n} x_i a_i = 1.$$

If we now define, for $t = 1, 2, \ldots, n$, homomorphisms f_t of I into R by $f_t(x) = xx_t$, then

$$\sum_t f_t(x)a_t = \sum_t xx_t a_t = x,$$

and so, by Proposition 1.35, I is projective.

Conversely, assume I to be projective. The previous proposition implies the existence of a set of elements $(a_t)_{t\in T}$ and homomorphisms $(f_t)_{t\in T}$ of I into R such that every element x of I can be written in the form

$$x = \sum_t f_t(x) a_t$$

with only a finite number of non-zero summands, Observe that for $x, y \in I$ we have

$$y f_t(x) = f_t(yx) = f_t(xy) = x f_t(y),$$

and so the ratio $x_t = f_t(x)x^{-1}$ is, for non-zero $x \in I$, an element of the quotient field K of R, independent of the choice of x. Moreover $x_t I \subset R$, thus $x_t \in I'$, and for any fixed $x \in I$ only finitely many elements $f_t(x) = x x_t$ are non-zero, whence only a finite number of x_t's do not vanish, say $x_1, \ldots, x_n$. Thus for any $x \in I$ we obtain an equality of the form

$$x = \sum_{t=1}^{n} f_t(x) a_t = \sum_{t=1}^{n} x x_t a_t = x \sum_{t=1}^{n} x_t a_t,$$

which implies

$$1 = \sum_{t=1}^{n} x_t a_t,$$

and so $R \subset II' \subset R$, i.e., $R = II'$ and I is invertible. □

Corollary. *In a Dedekind domains all non-zero ideals are projective.*

Proof : In fact, all non-zero ideals of R are invertible, □

To prove Theorem 1.32 we need two lemmas:

Lemma 1.37. *Let R be a domain in which every ideal is projective. If M is a finitely generated R-module contained in a free R-module F, then M can be represented as a direct sum of a finite number of ideals of R.*

Proof : Observe first that M is contained in a finitely generated free R-module. Indeed, if $a_1, \ldots, a_m$ generate M, then the set of free generators of F occurring in the canonical form of those elements is finite, and consists, say, of elements $x_1, \ldots, x_n$. The R-module generated by $x_1, \ldots, x_n$ is obviously free and contains M.

Now we apply induction in n. For $n = 0$ there is nothing to prove. Assume thus the truth of our lemma for all R-modules contained in a free R-module with $n-1$ free generators. Let M be a R-module contained in a free R-module F_n with n free generators $x_1, \ldots, x_n$, and let F_{n-1} be the free R-module generated by the first $n-1$ of them. Every element x of M can be written as $r_1 x_1 + \cdots + r_n x_n$ with $r_i \in R$, and the map $f : x \mapsto r_n$ is a homomorphism of M into R. Since the sequence

$$0 \longrightarrow \text{Ker } f \longrightarrow M \longrightarrow \text{Im } f \longrightarrow 0$$

is exact, and Im f is an ideal of R, projective by assumption, we may apply Proposition 1.34 to obtain $M \sim \text{Im } f \oplus \text{Ker } f$. This implies that Ker f is finitely generated, being a homomorphic image of M, and since Ker $f \subset F_{n-1}$, we may apply the inductional assumption to find that Ker f is a direct sum of ideals of R. Since Im f is also an ideal, the lemma follows. □

Lemma 1.38. *For every domain R any finitely generated and torsion-free R-module M is a submodule of a free R-module.*

Proof : Write $M = Rx_1 + \cdots + Rx_n$, and let K be the field of fractions of R. Then $Kx_1 + \cdots + Kx_n = M \otimes K$ is a finite-dimensional linear K-space. If $y_1, \ldots, y_m$ is its basis, then with suitable $r_{ij} \in K$ we may write

$$x_i = \sum_{j=1}^{m} r_{ij} y_j \quad (i = 1, 2, \ldots, n).$$

Now let q be a non-zero element of R satisfying $qr_{ij} \in R$ for all i and j. Then

$$M = Rx_1 + \cdots + Rx_n \subset Ry_1/q + \cdots + Ry_m/q,$$

and on the right-hand side of this inclusion we obviously have a free R-module. □

Proof of Theorem 1.32: Let M be a finitely generated module over a Dedekind domain R, and let A be its submodule consisting of all torsion elements of M. The factor-module $M_1 = M/A$ is torsion-free and finitely generated. Hence the Corollary to Proposition 1.36 and Lemmas 1.37, 1.38 imply that M_1 is a direct sum of ideals of R. The same corollary jointly with Proposition 1.33 shows that M_1 is projective, and so the exactness of the sequence

$$0 \longrightarrow A \longrightarrow M \longrightarrow M_1 \longrightarrow 0$$

gives, in view of Proposition 1.34, the decomposition

$$M \sim A \oplus M_1 \sim A \oplus I_1 \oplus \cdots \oplus I_m,$$

where $I_1, \ldots, I_m$ are ideals of R.

Now we prove that with a suitable ideal $I \subset R$ we have

$$I_1 \oplus \cdots \oplus I_m \sim R^{m-1} \oplus I.$$

For this purpose it suffices to show that for any pair J_1, J_2 of ideals of R there exists an ideal J such that $J_1 \oplus J_2 \sim R \oplus J$. First we show that there is an ideal J_1' of R which is isomorphic to J_1 as an R-module, and satisfies $(J_1', J_2) = R$. Choose $A \subset R$ so that the ideal $J_1 A = aR$ is principal and $(A, J_2) = R$, which is possible according to Corollary 6 to Proposition 1.14. Write $A = \prod_{i=1}^{t} P_i^{a_i}$, and choose $b \in R$ so that for $i = 1, 2, \ldots, t$ one has

$$b \in P_i^{a_i} \setminus P_i^{a_i+1}$$

and $b \equiv 1 \pmod{J_2}$. Then bR is divisible by A, hence we may write $bR = AJ_1'$ with some ideal J_1', relatively prime to J_2. Finally we get

$$aJ_1' = J_1 A J_1' = bJ_1,$$

which shows that $J_1 \sim bJ_1 = aJ_1' \sim J_1'$, as required.

Now consider the exact sequence

$$0 \longrightarrow J_1' \cap J_2 \longrightarrow J_1' \oplus J_2 \longrightarrow J_1' + J_2 \longrightarrow 0.$$

Since the ideals J_1' and J_2 are relatively prime, Proposition 1.13 (ii),(iii) shows that this sequence can be written as

$$0 \longrightarrow J_1' J_2 \longrightarrow J_1' \oplus J_2 \longrightarrow R \longrightarrow 0,$$

and the projectivity of R implies finally

$$J_1 \oplus J_2 \sim J_1' \oplus J_2 \sim R \oplus J_1' J_2$$

as asserted. As we have seen above, this establishes the theorem. □

Corollary. *Every non-zero finitely generated and torsion-free module over a Dedekind domain is projective.*

Proof : Follows from the theorem, Proposition 1.33 and the Corollary to Proposition 1.36.

2. Now we shall consider the question of uniqueness of the direct summands occurring in Theorem 1.32. Since the torsion submodule A is clearly unique, we may assume that our module is torsion-free.

Theorem 1.39. *If R is a Dedekind domain and M_1, M_2 are torsion-free R-modules written in the form*

$$M_1 = I_1 \oplus \cdots \oplus I_m, \quad M_2 = J_1 \oplus \cdots \oplus J_n,$$

where I_i, J_i are fractional ideals of R, then M_1 and M_2 are isomorphic if and only if $m = n$, and with a suitable element a of the field K of quotients of R one has

$$I_1 \cdots I_m = aJ_1 \cdots J_n.$$

Proof : The sufficiency of the condition given was already established in the last part of the proof of the preceding theorem. To prove its necessity assume that the modules M_1 and M_2 are isomorphic. The embedding of R in K induces an embedding of M_1 in K^m and of M_2 in K^n, and obviously M_1

spans K^m and M_2 spans K^n. The isomorphism of M_1 onto M_2 extends to a K-isomorphism of the spanned spaces, and so $m = n$.

To prove the remaining part of the theorem we assume that all ideals I_i, J_i contain the ring R. In fact, if I is one of those ideals, then with a suitable non-zero a in K we have, say, $R \subset aI = I'$. The mapping $x \mapsto ax$ shows that $I \sim I'$, whence

$$M_1 \sim I_1' \oplus \cdots \oplus I_m', \quad M_2 \sim J_1' \oplus \cdots \oplus J_m'.$$

If we prove the theorem in this case, then we shall have $I_1' \cdots I_m' = cJ_1' \cdots J_m'$ with some $c \in K$, and this obviously implies the equality $I_1 \cdots I_m = dJ_1 \cdots J_m$ with a suitable $d \in K$.

Now let f be an isomorphism of M_1 onto M_2, and let f_r be its restriction to I_r. If $1_r \in I_r$ is the unit element of R, then denote its image $f_r(1_r)$ by $[a_{r1}, \ldots, a_{rm}]$, with $a_{ri} \in J_i$ $(i = 1, 2, \ldots, m)$. We shall establish the equality

$$J_s = a_{1s}I_1 + \cdots + a_{ms}I_m \quad (s = 1, 2, \ldots, m).$$

Note first that if a, x and ax all lie in I_r, then $f_r(xa) = xf_r(a)$. Indeed, if $x = A/B$ with $A, B \in R$, then

$$Bf_r(ax) = Bf_r(aA/B) = f_r(aA) = Af_r(a),$$

hence

$$f_r(xa) = \frac{A}{B} f_r(a) = xf_r(a).$$

If we denote by p_s the projection of M_2 onto J_s, then in view of

$$f([x_1, \ldots, x_m]) = \sum_{i=1}^{m} f_i(x_i) = \sum_{i=1}^{m} x_i f_i(1_i),$$

we obtain the following chain of equalities:

$$\begin{aligned} \sum_{i=1}^{m} a_{is}I_i &= \left\{ \sum_{i=1}^{m} a_{is}x_i : \ x_i \in I_i \right\} \\ &= \{p_s(f_1(1_1)x_1 + \cdots + f_m(1_m)x_m) : \ x_i \in I_i\} \\ &= \{p_s(f([x_1, \ldots, x_m])) : \ x_i \in I_i\} = J_s. \end{aligned}$$

Now, if $C = \det[a_{ij}] = \sum_P \operatorname{sgn} P \cdot A_P$ is the expansion of the determinant of $[a_{ij}]$, then, multiplying all the equalities just obtained, we get

$$J_1 \cdots J_m = \prod_{s=1}^{m} \sum_{i=1}^{m} a_{is}I_i = \sum_P A_P I_1 \cdots I_m + \cdots,$$

which implies

$$\sum_P A_P I_1 \cdots I_m \subset J_1 \cdots J_m.$$

From this we shall now deduce the inclusion $CI_1 \cdots I_m \subset J_1 \cdots J_m$. Let P be any permutation of m letters, and let $x_i \in I_i$ for $i = 1, 2, \ldots, m$. If

$$y_i = \begin{cases} \operatorname{sgn} P \cdot x_1 & \text{for } i = 1, \\ x_i & \text{for } i = 2, \ldots, m, \end{cases}$$

then

$$A_P y_1 \cdots y_m = \operatorname{sgn} P \cdot A_P x_1 \cdots x_m \in A_P I_1 \cdots I_m \subset J_1 \cdots J_m,$$

and so the sum

$$\sum_P \operatorname{sgn} P \cdot A_P x_1 \cdots x_m,$$

which equals $Cx_1 \cdots x_m$, lies in $J_1 \cdots J_m$.

If we now exchange the roles of M_1 and M_2, we get $C_1 J_1 \cdots J_m \subset I_1 \cdots I_m$, where C_1 is the determinant of the matrix $[b_{ij}]$ defined by

$$g_r(e_r) = [b_{r1}, \ldots, b_{rm}],$$

where $e_r \in J_r$ is the unit element of R, and g_r is the restriction of g, the mapping inverse to f, to J_r. One sees easily that the matrices $[a_{ij}]$ and $[b_{ij}]$ are inverses of each other, and so $CC_1 = 1$, which at once implies the equality $I_1 \cdots I_m = C_1 J_1 \cdots J_m$. □

Corollary. *If A, B are ideals in a Dedekind domain R, and M is a finitely generated torsion-free R-module such that $A \oplus M$ and $B \oplus M$ are isomorphic, then A and B are isomorphic.*

Proof : Theorem 1.32 implies that $M \sim R^n \oplus I$ with a certain $n \geq 0$ and an ideal I of R, therefore

$$A \oplus R^n \oplus I \sim B \oplus R^n \oplus I,$$

and it suffices to apply Theorem 1.39. □

3. To conclude the study of finitely generated modules over Dedekind domains we shall now consider torsion modules, and start with the case of a principal ideal domain.

Proposition 1.40. *If R is a principal ideal domain and M is a finitely generated non-zero torsion R-module, then for some $n \geq 1$ there exist ideals $I_1, \ldots, I_n$ of R such that*

$$M \sim \bigoplus_{j=1}^{n} R/I_j.$$

Proof : For any non-zero prime ideal P of R denote by $M(P)$ the submodule of M consisting of all elements of M which are annihilated by some power of P, i.e.

$$M(P) = \{m \in M : \ P^r m = 0 \quad \text{for a certain } r \geq 1\}.$$

Since R is a principal ideal domain we have equivalently

$$M(P) = \{m \in M : \ \pi^r m = 0 \quad \text{for a certain } r \geq 1\},$$

where π is a generator of P. First we show that $M = \bigoplus_P M(P)$, where P runs over all prime ideals of R. Let $m \in M$ be non-zero, and let

$$\mathrm{Ann}(m) = \{r \in R : \ rm = 0\}$$

be its *annihilator*. It is a non-zero ideal, hence we can find irreducible elements $\pi_1, \ldots, \pi_s$ generating distinct prime ideals, and also exponents $\alpha_i \geq 1$ $(i = 1, 2, \ldots, s)$ so that $\mathrm{Ann}(m) = \pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s} R$. Since R is a principal ideal domain, and the elements

$$\rho_j = (\pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s})\pi_j^{-\alpha_j} \quad (j = 1, 2, \ldots, s)$$

do not have a non-unit common divisor, thus we may find $t_1, \ldots, t_s$ in R satisfying $\sum_{i=1}^{s} t_i \rho_i = 1$. This implies

$$m = \sum_{i=1}^{s} t_i \rho_i m \in \sum_{i=1}^{s} M(\pi_i R),$$

because $\rho_i m$ is annihilated by $\pi_i^{\alpha_i}$. This shows that $M = \sum_P M(P)$, but since only the zero element can be annihilated by two relatively prime elements, the sum $\sum_P M(P)$ is direct, and $M = \bigoplus_P M(P)$ follows. Since the Corollary to Proposition 1.2 implies that M is a Noetherian module, there can be only finitely many non-zero terms $M(P)$ in the sum in question.

It follows that it suffices to consider modules of the form $M(P)$ with a suitable prime ideal P. Note that for such modules M their annihilator

$$\mathrm{Ann}(M) = \bigcap_{m \in M} \mathrm{Ann}(m)$$

must be a power of P, because $\mathrm{Ann}(m)$ is a power of P for non-zero $m \in M$. Therefore, let $\mathrm{Ann}(M) = \pi^t R$, where π is a generator of P and $t \geq 1$. Let $m_1, \ldots, m_n$ be a set of generators of M. We use induction in the number n of generators. If $n = 1$, then M is an epimorphic image of R, and hence $M \sim R/I$ with a suitable ideal I of R. Assume now that our assertion holds for all modules having at most $n-1$ generators. Obviously at least one of the generators m_i satisfies $\mathrm{Ann}(m_i) = \pi^t R$, and we may assume that this holds for $i = n$. The factor-module $M/m_n R$ has less than n generators, whence we may write

$$M/m_n R = \bigoplus_{i=1}^{s} f(x_i)R,$$

where $x_1, \ldots, x_s$ are suitable elements of M, and $f : M \longrightarrow M/m_n R$ denotes the natural map. Put $\mathrm{Ann}(f(x_i)) = \pi^{r_i} R$ $(i = 1, 2, \ldots, s)$. Then $r_i \leq t$

and with suitable $k_i \geq 0$ and $a_i \in R \setminus \pi R$ we have $\pi^{r_i} x_i = \pi^{k_i} a_i m_n$ $(i = 1, 2, \ldots, s)$.

Because of

$$0 = \pi^t x_i = \pi^{t-r_i+k_i} a_i m_n$$

we infer that $k_i \geq r_i$. Putting $y_i = x_i - \pi^{k_i - r_i} a_i m_n$, we obtain $\pi^{r_i} y_i = 0$ and $f(y_i) = f(x_i)$. This gives

$$\mathrm{Ann}(f(x_i)) = \pi^{r_i} R \subset \mathrm{Ann}(y_i) \subset \mathrm{Ann}(f(y_i)) = \mathrm{Ann}(f(x_i)),$$

thus $\mathrm{Ann}(f(y_i)) = \mathrm{Ann}(y_i)$. It follows that the restriction of the map f to $y_i R$ is an isomorphism for $i = 1, 2, \ldots, s$, and because of

$$f(y_1 R + \cdots + y_s R) = M/m_n R = \bigoplus_{i=1}^{s} f(y_i) R$$

f maps $y_1 R + \cdots + y_s R$ isomorphically onto $\bigoplus_{i=1}^{s} f(y_i) R$, and so the sum $\sum_{i=1}^{s} y_i R$ is direct. This leads to

$$M = m_n R \oplus \bigoplus_{i=1}^{s} y_i R,$$

and applying the inductional assumption we arrive at our assertion. □

Using the proposition just proved, we can now describe all finitely generated torsion modules over a Dedekind domain. It turns out that their structure is not more complicated than in the case of a principal ideal domain.

Theorem 1.41. *If R is a Dedekind domain and M a non-zero finitely generated and torsion R-module, then there exist ideals $I_1, \ldots, I_n$ of R such that*

$$M \sim \bigoplus_{j=1}^{n} R/I_j.$$

Proof : The set $I = \{r \in R : \ rm = 0 \quad \text{for all } m \in M\}$ is a non-zero ideal in R, and we can regard M as an R/I module via

$$r \,(\mathrm{mod}\ I) \cdot m = rm \quad (r \in R, m \in M).$$

Write

$$I = \prod_{j=1}^{t} P_j^{\alpha_j}$$

with distinct prime ideals $P_1, \ldots, P_t$ and $\alpha_j \geq 1$. Theorem 1.15 implies

$$R/I \sim \bigoplus_{j=1}^{t} R/P_j^{\alpha_j},$$

and to utilize this decomposition we need the following auxiliary result:

Lemma 1.42. *If a commutative ring S with unit e is a direct sum of its subrings S_j (with units e_j)*

$$S = \bigoplus_{j=1}^{t} S_j,$$

then every S-module M can be written in the form

$$M = \bigoplus_{j=1}^{t} M_j,$$

where $M_1, \ldots, M_t$ are S-modules, and for $i \neq j$ and $s_i \in S_i$ we have $s_i M_j = 0$.

Proof : Clearly we have $e = e_1 + \cdots + e_t$. Put $M_j = e_j M$ for $j = 1, 2, \ldots, t$. Then for $i \neq j$ and $s \in S_j$ we have $sM_i = 0$. Since for a in M

$$a = e_1 a + \cdots + e_t a \tag{1.7}$$

and $e_j a \in M$, the sum of the modules M_j equals M, and it remains to show that this sum is direct, i.e., the decomposition (1.7) is unique. This can be seen in the following way: if $a = m_1 + \cdots + m_t$ with $m_i \in M_i$ $(i = 1, 2, \ldots, t)$, then $m_i = e_i x_i$ for suitable $x_i \in M_i$, thus

$$e_j a = \sum_{i=1}^{t} e_j m_i = \sum_{i=1}^{t} e_j e_i x_i = e_j^2 x_j = e_j x_j = m_j,$$

hence our decomposition coincides with (1.7). □

We apply the lemma for $S = R/I$, $S_j = R/P_j^{\alpha_j}$, and obtain the equality

$$M = \bigoplus_{j=1}^{t} M_j,$$

where each M_j can be regarded as an $R/P_j^{\alpha_j}$-module, and for $i \neq j$ one has $(R/P_j^{\alpha_j})M_i = 0$.

To conclude the proof it is sufficient to show that every finitely generated R/P^{α}-module N (where P is a prime ideal of R and $\alpha \geq 1$) is isomorphic to the direct sum $\bigoplus_{j=1}^{t} R/P^{\beta_j}$ with a certain $t \geq 0$ and $1 \leq \beta_j \leq a$. If R_P denotes the valuation ring induced by the P-adic valuation, then by Proposition 1.27 (iv) the rings R/P^{α} and $R_P/(PR_P)^{\alpha}$ are isomorphic. Thus N becomes an R_P-module with the property $(PR_P)^{\alpha} N = 0$. Since by Theorem 1.26 R_P is a principal ideal domain, Proposition 1.40 is applicable, and we see that

$$N \sim \bigoplus_{j=1}^{t} R_P/I_j$$

with suitable ideals I_j of R_P. Theorem 1.26 implies that each I_j is a power or PR_P, and owing to $(PR_P)^\alpha N = 0$ we must have $I_j = (PR_P)^{\beta_j}$ with $1 \leq \beta_j \leq \alpha$. Since $R \subset R_P$, we can regard R_P/I_j as an R-module, and since the ring-isomorphism of R/P^{β_j} and $R_P/(PR_P)^{\beta_j}$ is also an R-module isomorphism, we obtain finally

$$N \sim \bigoplus_{j=1}^{t} R/P^{\beta_j},$$

as asserted. □

4. We conclude this chapter with the introduction of the notion of the *class-group of a Dedekind domain*, which will play an important role in the sequel. Its definition is based on the following simple result:

Proposition 1.43. *If R is a Dedekind domain and $I_1 \sim I_2$, $J_1 \sim J_2$ are two pairs of its fractional ideals, which are isomorphic as R-modules, then the products I_1J_1 and I_2J_2 are also isomorphic.*

Proof : Since obviously $I_1 \oplus J_1 \sim I_2 \oplus J_2$, Theorem 1.39 implies the existence of a non-zero $a \in K$, the field of fractions of R, such that $I_1J_1 = aI_2J_2$, and this shows that the map $x \mapsto ax$ of I_2J_2 onto I_1J_1 is an isomorphism. □

This proposition implies the compatibility of the multiplication of ideals with the partition of all fractional ideals into classes of isomorphic ideals, and so permits us to define a multiplication in the set of these classes in the following way: if $c(I), c(J)$ are classes containing I and J, respectively, then their product is defined by $c(I)c(J) = c(IJ)$. This induces a semigroup structure in the set of classes, but one sees easily that it is in fact a group structure, because the existence of inverses is implied by the invertibility of fractional ideals.

The resulting group is called the *group of ideal classes of R*, or simply the *class-group of R*, and is usually denoted by $H(R)$. If it is finite, then the number of elements of $H(R)$ is called the *class-number of R* and denoted by $h(R)$.

For further reference we point out a simple result:

Proposition 1.44. *Every class of ideals contains an ideal of R.*

Proof : If I is a fractional ideal and $c \in R$ is non-zero and satisfies $cI \subset R$, then I and cI lie in the same class. □

The importance of the class group is explained by the following result:

Theorem 1.45. *If R is a Dedekind domain, then the following statements are equivalent:*

(i) $H(R)$ is the trivial group, i.e., $h(R) = 1$,

(ii) R is a principal ideal domain (PID),

(iii) R is a unique factorization domain (UFD).

Proof : If $H(R)$ is trivial, then every non-zero ideal of R is isomorphic to R as an R-module, hence has the form aR with a certain non-zero $a \in R$, This establishes the implication (i)$\rightarrow$ (ii). The implication (ii)$\rightarrow$(iii) being clear, assume that R is a unique factorization domain. We show first that every irreducible element of R (i.e., a non-zero and non-invertible element which does not have proper divisors) generates a prime ideal. If a is irreducible and $aR = P_1 \cdots P_s$ with $s \geq 2$, then by Corollary 5 to Proposition 1.14 we get

$$P_i = a_i R + b_i R = (a_i R, b_i R) \quad (i = 1, 2, \ldots, s)$$

with suitable $a_i, b_i \in R$. For every i we have either $a \nmid a_i$ or $a \nmid b_i$, and we may assume that $a \nmid a_i$ holds for $i = 1, 2, \ldots, s$. However, $a_1 \cdots a_s \in P_1 \cdots P_s = aR$, thus a divides the product $a_1 \cdots a_s$ without dividing any of its factors, which is impossible for an irreducible element in a UFD.

This shows that irreducible elements generate prime ideals. If $H(R)$ were non-trivial, there would exist at least one non-principal prime ideal, say P, because otherwise all ideals would be principal. Write $P = (aR, bR)$ with suitable $a, b \in R$, and factorize a into irreducibles, say $a = a_1 \cdots a_r$. Since the ideals $a_i R$ are prime, it follows that for a certain i we have $a_i R = P$, thus P is principal, contrary to our assumption. This establishes the implication (iii)$\rightarrow$(i). □

1.4. Notes to Chapter 1

1. The theory of Dedekind domains was created as a generalization of results concerning rings of integers in finite extensions of the rationals, obtained mainly by Dedekind [71]. It was observed already by Dedekind and H.Weber [82] that many of these results apply also to the rings of integral elements in function fields. However, the general theory had to wait for the introduction of abstract methods and concepts into algebra. In fact, the definition of an abstract ring, in the form used today, appears for the first time in Fraenkel [16], and the definition of an abstract field is not much older (Steinitz [10]).

The role of the ascending chain condition for ideals (the Noether condition) for the theory of commutative rings was emphasized by Noether [21]. She obtained the fundamental results for Noetherian rings, generalizing many

earlier results obtained for polynomial rings by Hilbert [90], Lasker [05] and Macaulay [13], [16].

The presented by us standard proof of Proposition 1.1 uses the axiom of choice; in fact, as shown in Hodges [74], this cannot be avoided.

The theory of rings, now called Dedekind domains, originated with Noether [27a] (preceded by Noether [19]) where the condition which is both necessary and sufficient for a domain R to have unique factorization of ideals into prime ideals was given in the following form: R should be Noetherian and integrally closed, and for every non-zero ideal I of R the factor-ring R/I should be *Artinian*, i.e., it should satisfy the descending chain condition for ideals. The last condition is also called the *restricted minimum condition*. The equivalence of these definition to the definition given by us was established by Nakano [43], and a simple proof was given by I.S.Cohen [50]. See also Krull [28a].

The proof of Theorem 1.5 shows that any invertible ideal in a domain is finitely generated, a fact first noted by Krull [30].

The existence of factorization of all non-zero proper ideals into prime ideals implies its uniqueness. This is implicit in Mori [40], but apparently the first explicit mention was made in Matusita [44]. Here again for a simple proof the reader is referred to I.S.Cohen [50] (cf. Butts [64]).

2. Theorem 1.8 gives one of several known characterizations of Dedekind domains. Apparently it was first formulated in the second volume of van der Waerden [30], although its essence is contained already in Noether [27a]. Let us quote some other characterizations of Dedekind domains:

(i) A domain is Dedekind if and only if the non-zero fractional ideals form a group under multiplication (Krull [35], p.13, "Gruppensatz").

(ii) A domain R is Dedekind if and only if for every proper non-zero ideal I of R the factor ring R/I is a unique factorization ring (Jensen [63]).

(iii) A domain satisfying the (FN) condition is Dedekind if and only if Theorem 1.16 (i) holds in it (Butts, Wade [66]).

In the books of Fossum [73], Gilmer [68] and Larsen and McCarthy [71] one finds several other characterizations of Dedekind domains. Later new characterizations were given in Hays [73], Huckaba, Papick [81], Idelhadj, Yahya [00], Koyama, Nishi, Yanagihara [74], Lequain [85], Man [98] and Quadri, Irfan [79].

Characterizations of domains whose integral closure in its field of fractions is Dedekind were given in Butts, W.W.Smith [66] and Dumitrescu, Shah, Zafrullah [00].

3. For the history of Proposition 1.13 see Dedekind [95].

Noetherian rings in which every ideal is generated by at most k elements (with fixed k) were considered in I.S.Cohen [50] and Gilmer [72],[73]. Matlis [70] characterized domains in which every ideal is generated by at most two elements. The first example of a domain with an invertible ideal having k, but

not fewer, generators was given by Chase, and the first published example appeared in Gilmer [69].

An early study of invertible ideals appears in W.Weber [31].

Theorem 1.20 was proved in full generality in Noether [27a], and in the habilitation thesis of F.K.Schmidt in 1927 (cf. Grell [36a]). F.K.Schmidt [36] gave an example marking the important distinction between the separable and inseparable case. Another proof of Theorem 1.20 was given in Northcott [55]. For infinite extensions this theorem ceases to be true. Indeed, the ring of all algebraic integers, which is the integral closure of $\mathbb{Z}$ in the field of all algebraic numbers, is not even Noetherian.

Of the several books concerning ideals in commutative rings we mention only the classical works of Krull [35], Bourbaki [61/65] and Zariski, Samuel [58], as well as a few later books: Gilmer [68], Kaplansky [70], Larsen, McCarthy [71].

4. Valuations were introduced by Kürschak [13], and the main results of their theory were established by Ostrowski [13],[17],[18],[35] and Krull [31]. An account of this theory may be found in Schilling [50] and Ribenboim [99]. For its history see Roquette [02].

Theorem 1.31 is due to Ostrowski [18], who also described valuations of algebraic number fields (see Theorem 3.3), The reproduced proof is that of Artin [32b].

Theorems 1.32, 1.39 and 1.41 are essentially due to Steinitz [12], who considered rings of integers in algebraic number fields. The presented proof of the necessity part of Theorem 1.39 is due to Kaplansky [52]. It works for an arbitrary integral domain. Cf. Archinard [84], Asano [50], Chevalley [36b].

Theorem 1.32 implies that if every finitely generated module over a Dedekind domain R is a direct sum of cyclic modules (i.e., generated by one element), then R is a PID. Rings having this property are called *FGC–rings*. For characterizations of these rings see Brandal [79], Kaplansky [49], Lafon [71], Vámos [70], Wiegand, Wiegand [77]. Uzkov [63] showed that a Noetherian FGC-domain must be a unique factorization domain (cf. Bass [62]).

Theorem 1.32 has its analogue for projective modules over the group ring $R[G]$ of a finite group G in the case, when R is Dedekind (Swan [60], Giorgiutti [60]). For a discussion of free modules over a Dedekind domain see O'Meara [56].

5. The notion of class-group goes back to Kummer [47b] in the case of integer rings in cyclotomic fields, and even to Gauss [01] in the case of quadratic fields. Gauss dealt with classes of quadratic forms, but his theory is equivalent to the theory of ideal classes in quadratic fields, as we shall see in Chap. 8.

Analogues of the class-group were defined also in other situations (Grothendieck group, Picard group,...). See e.g. Bass [68], Claborn, Fossum [68], Fossum [73], Kennedy [80], Milnor [71], Reyes Sanchez [99], Serre [58], Ullom [76].

An old conjecture that every Abelian group may serve as a class-group for a suitable Dedekind domain was settled affirmatively by Claborn [66]. A proof may be found in Fossum [73], and another proof was provided by Leedham–Green [72]. For an extension see Claborn [68] (cf. Grams [74]). If the group in question is finitely generated that one can find a suitable Dedekind domain R satisfying $\mathbb{Z}[X] \subset R \subset \mathbb{Q}[X]$ (Eakin, Heinzer [73]).

It has been also conjectured (see Zariski, Samuel [58]) that every Dedekind domain is the integral closure of a principal ideal domain in a finite extension of its quotient field. However this conjecture was disproved by Claborn [65] (for a simple example see Adachi [85]). He suggested in turn, that every Dedekind domain can be represented as the ring of quotients of such an integral closure with respect to a subset closed under multiplication. However, this conjecture also fails (Leedham-Green [72]), and the question whether one can construct every Dedekind domain in a simple fashion starting with PID's remains still unanswered.

EXERCISES

1. Let R be a commutative ring with unit, and let I, J be ideals in R. Prove that if R/I and R/J are isomorphic as R-modules, then $I = J$, and show that this implication may fail if we replace R-module isomorphism by ring isomorphism.

2. Show that a domain R is Dedekind if and only if its fractional ideals form a group under multiplication.

3. Prove that if M is a finitely generated module over a Noetherian ring, then M is a Noetherian module.

4. Let I be a fractional ideal of a domain R. Prove that I is invertible if and only if there exists a fractional ideal J such that IJ is principal.

5. (i) Prove that if in a domain R all proper non-zero ideals are either prime or can be represented uniquely as products of prime ideals, then R is Dedekind.

(ii) Show that in (i) one can omit the uniqueness assumption.

6. Prove that if R is a Dedekind domain and I is a non-zero ideal in R, then the ring R/I is Artinian.

7. (Camion, Levy, Mann [73]) Let R be an integral domain in which every finitely generated ideal is invertible (such domains are called *Prüfer domains*). Prove the following three assertions:

(i) If I is a finitely generated ideal of R, and for certain ideals A, B we have $AI = BI$, then $A = B$.

(ii) If I is a finitely generated ideal of R, and J is an ideal contained in I, then there exists an ideal A with $AI = J$.

(iii) If A, B, C are finitely generated ideals of R, then $A \cap (B+C) = A \cap B + A \cap C$.

8. Let R be a Dedekind domain, I a non-zero ideal of R and $N \geq 1$. Prove that if $R^{N-1} \oplus I$ can be generated by N elements, then I is principal.

9. (Reiner [56] in case $d = 1$, Moore [75] in the general case) Let R be a Dedekind domain, Prove that if $a_1, \ldots, a_n$ in R are given, and d lies in the R-module generated by the a_i's, then there exists an $n \times n$ invertible matrix with entries in R and determinant d, whose first row equals $a_1, a_2, \ldots, a_n$.

10. Let R be a Dedekind domain, $G(R)$ the group of all its fractional ideals and $P(R)$ the group of all principal fractional ideals. Prove that the quotient group $G(R)/P(R)$ is isomorphic to the class-group of R.

2. Algebraic Numbers and Integers

2.1. Distribution of Integers in the Complex Plane

1. In this chapter we introduce the fundamental notions of the theory, and develop some of their properties. Let us start with definitions. Any complex number which is integral over the field $\mathbb{Q}$ of rational numbers will be called an *algebraic number*, and if it is also integral over the ring $\mathbb{Z}$ of rational integers, then it will be called an *algebraic integer*. Corollary to Proposition 1.6 shows that the set of all algebraic numbers forms a ring, and the same holds for the set of all algebraic integers. Actually the first of these rings is a field, since if $a \neq 0$ is algebraic, then it is a root of $X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$ with rational a_i's and non-zero a_0, hence a^{-1} is a root of the polynomial $X^m + a_0^{-1}a_1X^{m-1} + \cdots + a_0^{-1}$.

The minimal degree of a non-zero polynomial over $\mathbb{Q}$ whose root is a is called the *degree of* a. We shall denote it by $\deg a$, or $\deg_{\mathbb{Q}} a$. If K is any subfield of the field $\mathbb{C}$ of complex numbers, then $\deg_K a$, the *degree of* a *over* K, is defined as the minimal degree of a non-zero polynomial with coefficients in K, having a for one of its roots. This polynomial is called the *minimal polynomial of* a *over* K, provided it is monic, i.e., its leading coefficient equals 1.

Any finite extension of $\mathbb{Q}$ will be called an *algebraic number field*. By Corollary to Proposition 1.6, the algebraic integers contained in such field K form a ring, which we shall denote by R_K. The elements of this ring will be called the *integers of* K, and our chief aim is to study their properties, as well as the properties of the ring R_K as a whole. Note that every algebraic number field K can be written in the form $K = \mathbb{Q}(a)$ with a suitable a, which can be taken from R_K. This implies that every element of K is of the form $P(a)$, where P is a polynomial over $\mathbb{Q}$ of degree smaller than $\deg a = [K : \mathbb{Q}]$, the degree of K. The naive hope that with a suitable choice of a one may be able to write every integer of K in the form $P(a)$ with $P \in \mathbb{Z}[X]$ is unjustified, as will be shown on examples later on.

It will be useful to note at this point that R_K, being the integral closure of $\mathbb{Z}$ in K is, by Theorem 1.7, also the integral closure of the ring R_L for every subfield L of K.

If K/k is an extension of degree n, $a \in K$ and $F \in k[X]$ is the minimal polynomial of a, then the roots $a = a_1, \ldots, a_n$ of F are called the *conjugates*

of a over k. Note that if a generates the field K over k, i.e. $K = k(a)$, then the mappings F_i, defined for $i = 1, 2, \ldots, n$ by

$$F_i(\sum_{j=0}^{n-1} A_j a^j) = \sum_{j=0}^{n-1} A_j a_i^j \quad (A_0, A_1, \ldots, A_{n-1} \in K)$$

are isomorphisms of K into its integral closure, which are identities on k, and every such isomorphism must be of this form, since the image of a under it has to coincide with one of the a_i's. This shows that in case of $k = \mathbb{Q}$ we get exactly $n = [K : \mathbb{Q}]$ different embeddings of K into the field of complex numbers.

The fields $F_i(K)$ are called the *fields conjugated to K*. Obviously, if we consider K as a subfield of the algebraic closure of K, then one of the F_i's is the identity on K.

Observe that if b is an arbitrary element of K, not necessarily generating it, then its images $F_i(b)$ must be conjugated to b, and it is easy to see that if the degree of b is smaller than the degree of K, then these images cannot be all distinct.

In the case of algebraic number fields one calls an embedding F_i *real* if $F_i(K)$ is contained in the real field $\mathbb{R}$, and is called *complex* (or *imaginary*) otherwise. Note that if F_i is a complex embedding, then its complex conjugate is again a complex embedding distinct from F_i, hence the number of complex embeddings is always even. One half of this number is usually denoted by $r_2 = r_2(K)$, and the number of real embeddings by $r_1 = r_1(K)$. The pair $[r_1(K), r_2(K)]$ is called the *signature of K*. The equality $r_1(K) + 2r_2(K) = [K : \mathbb{Q}]$ is obvious.

Fields K with $r_2(K) = 0$ are called *totally real*, and fields with $r_1(K) = 0$ *totally complex* or *totally imaginary*[1]. Note that if the extension $K/\mathbb{Q}$ is Galois, then K is either totally real or totally imaginary, since all images $F_i(K)$ have to coincide.

Usually one fixes the order of the embeddings $F_1, \ldots, F_n$ in such a way that $F_1, \ldots, F_{r_1}$ are real, the remaining embeddings are complex, and, moreover, for $i = r_1 + r_2 + 1, \ldots, n$ one has $F_i = \bar{F}_{i-r_2}$. In the sequel we shall always assume tacitly that the embeddings are ordered in this way.

An algebraic number is called *totally real* if all its conjugates are real, and *totally complex* if none of them is real.

The product or r_1 copies of the multiplicative group $\{-1, 1\}$ is called the *signature group* of K and denoted by $Sgn(K)$. There is a canonical homomorphism (the *signature map*) $Sgn : K^* \to Sgn(K)$, defined by $Sgn(a) = [\epsilon_1, \ldots, \epsilon_{r_1}]$, where ϵ_i is the sign of $F_i(a)$. The elements of the kernel of the signature map are called *totally positive numbers*. One writes $a \gg 0$ to indicate that a is totally positive. Note that this notion depends on

[1] Observe that totally positive fields exist only in the MOS classification, but not in nature.

K, since in a totally complex field all non-zero numbers are totally positive, and in particular such are all negative rationals, which are certainly not positive in any real field. Clearly all non-zero squares of K and their sums are totally positive, and it follows from a result of Siegel [21b] that conversely, every totally positive element of K is a sum of squares of elements of K. In fact Siegel established that four square summands suffice.

2. The signature map is surjective. To prove this we need a simple lemma, which will be also used later:

Lemma 2.1. *Let K be a field of degree n and signature $[r_1, r_2]$. Put $k = r_1 + r_2$, and let $F_1, \dots, F_k$ be the embeddings of K into $\mathbb{C}$, the first r_1 of them being real, and from every pair of conjugate complex embeddings only one being taken. The map $\Psi : R_K \longrightarrow \mathbb{R}^n$ defined by*

$$\Psi : \ x \mapsto [F_1(x), \dots, F_{r_1}(x), \mathrm{Re}F_{r_1+1}(x), \mathrm{Im}F_{r_1+1}(x), \dots, \\ , \dots, \mathrm{Re}F_{r_1+r_2}(x), \mathrm{Im}F_{r_1+r_2}(x)]$$

is an injective homomorphism of the additive group of R_K in $\mathbb{R}^n$, and its image is an n-dimensional lattice, i.e. a free Abelian subgroup of $\mathbb{R}^n$ with n free generators.

Proof : Injectivity of Ψ results from the fact that $\Psi(x) = 0$ implies $x = 0$. Observe that the image $\Lambda = \Psi(R_K)$ is not dense in $\mathbb{R}^n$. Indeed, the set

$$A = \{[x_1, \dots, x_n] : \ |x_i| < 1/2 \text{ for } i = 1, 2, \dots, n\}$$

cannot contain non-zero points of Λ, since if x is a non-zero element of R_K with $\Psi(x) \in A$, then $|F_i(x)| < 1$, and therefore the product of all conjugates of x, which must be a non-zero rational integer, turns out to be of absolute value less than 1.

Thus Λ is a discrete subgroup of $\mathbb{R}^n$, hence it must be isomorphic to $\mathbb{Z}^d$ with a suitable $0 \leq d \leq n$. To show that $d = n$ it suffices to establish n linearly independent points in Λ, and here we may take the images of $1, u, u^2, \dots, u^{n-1}$, where u is any integer of K of degree n. In fact, if with real $A_0, \dots, A_{n-1}$ one has

$$\sum_{j=0}^{n-1} A_j \Psi(u^j) = 0,$$

then for $k = 1, 2, \dots, n$

$$\sum_{j=0}^{n-1} A_j F_k(u^j) = 0$$

follows. Since the determinant of the matrix $[F_k(u^j)]_{j,k}$ does not vanish, being a Vandermonde determinant, we obtain $A_0 = A_1 = \cdots = A_{n-1} = 0$. □

We prove now two results about the existence of elements with certain properties in every residue class mod I.

Proposition 2.2. *Let I be a non-zero ideal in R_K, and let X be one of residue classes* mod I.

(i) There exist infinitely many elements of X with an arbitrary prescribed signature.

(ii) There exist infinitely many elements of X, which generate the extension $K/\mathbb{Q}$.

Proof : (i) If $r_1 = 0$, then $Sgn(K) = \{1\}$ and there is nothing to prove. So assume $r_1 \geq 1$ and let $\epsilon = [\epsilon_1, \ldots, \epsilon_{r_1}] \in Sgn(K)$ be given. We prove first the existence of an integer $b \in K$ with $Sgn(b) = \epsilon$. If Ψ is the mapping defined in the preceding lemma, then $\Lambda = \Psi(R_K)$ has infinitely many points in each of the 2^{r_1} parts into which the hyperplanes $x_i = 0$ $(i = 1, 2, \ldots, r_1)$ divide $\mathbb{R}^n$. This proves the existence of $b \in R_K$ with $Sgn(b) = \epsilon$. If now $a \in I$ is totally positive (we may take $a = N(I)$, for example), then the numbers $abk + x$ $(x \in X,\ k = 1, 2, \ldots)$ are all in X, and for sufficiently large k satisfy

$$Sgn(abk + x) = Sgn(ab) = Sgn(b) = \epsilon.$$

(ii) Put $N = N(I)$, choose an element $a \in X$, and let $b \in R_K$ be any generator of $K/\mathbb{Q}$. Since $N \in I$, all elements $c_m = a + mNb$ $(m = 1, 2, \ldots)$ lie in X. If none of them generates K, then for every m there exist $i \neq j$ such that $F_i(c_m) = F_j(c_m)$. Hence there are indices $i_0 \neq j_0$ such that the equality $F_{i_0}(c_m) = F_{j_0}(c_m)$ holds for infinitely many m, but in view of $F_{i_0}(b) \neq F_{j_0}(b)$ this can happen only for

$$m = \frac{F_{j_0}(a) - F_{i_0}(a)}{(F_{i_0}(b) - F_{j_0}(b))N},$$

a contradiction. □

To prove the existence of fields with prescribed signature we need to show that the roots of a complex polynomial depend continuously on its coefficients.

Lemma 2.3. *Let $P(X) = X^n + \sum_{j=0}^{n-1} a_j X^j$ be a polynomial with complex coefficients, and denote by $z_1, z_2, \ldots, z_n$ its roots. Assume that they are all distinct. Let also $P_k(X) = X^n + \sum_{j=0}^{n-1} a_j^{(k)} X^j$ $(k = 1, 2, \ldots)$ be a sequence of polynomials satisfying $\lim_{k\to\infty} a_j^{(k)} = a_j$, and let $w_1^{(k)}, \ldots, w_n^{(k)}$ be the roots of P_k. Then it is possible to reorder those roots in such a way that for every $\epsilon > 0$ and sufficiently large k one has*

$$|z_i - w_i^{(k)}| < \epsilon.$$

Moreover, if the coefficients of P and P_k are real, then for sufficiently large k the polynomials P and P_k have the same number of real zeros.

Proof : Observe first that there is a common bound for the numbers $w_j^{(k)}$, and renumber them in the following way: let $w_1^{(k)}$ be the root of P_k, which is closest to z_1. If there are several such roots, then choose one of them arbitrarily. Of the remaining roots of P_k let $w_2^{(k)}$ be the closest to z_2, and continue this process. Next choose a sequence $k_1 < k_2 < \dots$ of integers such that the limit

$$c_j = \lim_{r\to\infty} w_j^{(k_r)}$$

exists for $j = 1, 2, \dots, n$. Then

$$P(X) = \lim_{r\to\infty} P_{k_r}(X) = \lim_{r\to\infty} \prod_{i=1}^{n} (X - w_i^{(k_r)}) = \prod_{i=1}^{n} (X - c_i),$$

and therefore the sets $\{z_1, \dots, z_n\}$ and $\{c_1, \dots, c_n\}$ coincide.

Moreover, $|w_1^{(k_r)} - z_1| \le |w_i^{(k_r)} - z_1|$ for $i = 2, 3, \dots, n$, thus $|c_1 - z_1| \le |c_i - z_1|$, and $c_1 = z_1$ follows. In the same manner one proves $c_i = z_i$ for all i. Finally note that the sequence k_r could be chosen arbitrarily, provided the required limit exists, and so $\lim_{k\to\infty} w_i^{(k)} = z_i$ holds for $i = 1, 2, \dots, n$, proving the first part of the lemma.

To prove the second part, note that if the coefficients of P and P_k are real, z_i is a real root of P, and for an infinite sequence $\{k_r\}$ the numbers $w_i^{(k_r)}$ are not real, then the numbers $\overline{w_i^{(k_r)}}$ are also roots of P_k, and so, by the foregoing argument, they tend to a root of P, say z_j, distinct from z_i, which is impossible, since

$$z_j = \lim_{r\to\infty} \overline{w_i^{(k_r)}} = \bar{z}_i = z_i,$$

z_i being real. □

Corollary. *There exist finite extensions of the rationals with the signature $[r_1, r_2]$ arbitrarily given.*

Proof : Take an arbitrary monic polynomial P with real coefficients, having r_1 real and $2r_2$ non-real roots, none of them multiple. Then choose a sequence of monic polynomials with coefficients of the form $(4k + 2)/(2m + 1)$, with $k, m \in \mathbb{Z}$, tending to P. Lemma 2.3. shows that if these polynomials are sufficiently close to P, then they have r_1 and $2r_2$ non-real roots, and since Eisenstein's criterion shows that they are all irreducible over the rationals, the fields generated by their roots have the required signature. □

3. Let K be a field of zero characteristic, and let L/K be an extension of degree n, contained in an algebraic closure Ω of K. Let $F_1, \ldots, F_n$ be the embeddings of L in Ω, which are identities on K. For $a \in L$ define the *characteristic polynomial* Φ_a of a over K by putting

$$\Phi_a(X) = \prod_{i=1}^{n}(X - F_i(a)).$$

One sees immediately that the coefficients of Φ_a lie in K, and if $f_a \in K[X]$ is the minimal polynomial of a over K, and $\deg_K a = m$, then $\Phi_a(X) = f_a(X)^{n/m}$.

There are two important mappings, connected with coefficients of characteristic polynomials: the *norm*

$$N_{L/K}(a) = \prod_{i=1}^{n} F_i(a) = (-1)^n \Phi_a(0),$$

and the *trace*, defined by

$$T_{L/K}(a) = \sum_{i=1}^{n} F_i(a).$$

Note that the trace of a differs only in sign from the coefficient of X^{n-1} in the characteristic polynomial of a.

The following proposition exhibits their principal proprieties:

Proposition 2.4. (i) *The norm $N_{L/K}$ is a homomorphism of L^*, the multiplicative group of L, into K^*, and the trace $T_{L/K}$ is a homomorphism of the corresponding additive groups.*

(ii) *The norm and the trace of an algebraic integer are algebraic integers.*

(iii) *If the extensions L/K and M/L are finite, then*

$$N_{M/K} = N_{L/K} \circ N_{M/L}, \quad T_{M/K} = T_{L/K} \circ T_{M/L}.$$

Proof : Assertion (i) is an immediate consequence of the definition, and to establish (ii) observe that the coefficients of the characteristic polynomial of an algebraic integer $a \in L$ lie in the ring generated by the coefficients of the minimal polynomial of a.

To prove (iii) let $m = [L : K]$, $n = [M : L]$, and let $s_1, \ldots, s_m$ be the embeddings of L into Ω which are equal to the identity on K, and extend them to embeddings of Ω into Ω. Moreover let $t_1, \ldots, t_n$ be embeddings of M into Ω, which are equal to the identity on L, and again extend them to the whole field Ω. If s is an embedding of M into Ω, equal to the identity on K, then with a suitable j we have $s_j^{-1} \circ s(L) = K$, and so for a certain i

we have $s_j^{-1} \circ s = t_i$. This shows that every embedding of M into Ω, which equals the identity on K, has the form $s_j \circ t_i$, and hence for $x \in M$ we get

$$N_{M/K}(x) = \prod_{i,j} s_j \circ t_i(x) = \prod_{j=1}^{m} s_j(\prod_{i=1}^{n} t_i(x))$$
$$= \prod_{j=1}^{m} s_j(N_{M/L}(x)) = (N_{L/K} \circ N_{M/L})(x),$$

as asserted. The same argument applies to the trace mapping (it suffices to replace each product by a sum, and write T in place of N). □

4. The earliest result concerning the distribution of algebraic integers in the complex plane is due to Kronecker [57a], and, with the use of the notation $\overline{|a|}$ for the largest absolute value of conjugates of a over $\mathbb{Q}$, runs as follows:

Theorem 2.5. (i) *If $a \neq 0$ is an algebraic integer which is not a root of unity, then $\overline{|a|} > 1$.*

(ii) *If $a \neq 0$ is a totally real integer which is not of the form $2\cos(\pi r)$ with rational r, then $\overline{|a|} > 2$.*

Proof : (i) Let a be a non-zero algebraic integer and assume that $\overline{|a|} \leq 1$. Let $K = \mathbb{Q}(a)$ and $n = [K : \mathbb{Q}]$. The numbers $a, a^2, \ldots$ all lie in R_K, therefore their minimal polynomials have degrees not exceeding n. Since all conjugates of the numbers a^k lie in the closed unit disc, the coefficients of their minimal polynomials do not exceed $\max\{\binom{n}{j} : j = 1, 2, \ldots, n\}$. This shows that the sequence $a, a^2, \ldots$ contains only finitely many distinct terms, and so for certain $i \neq j$ we have $a^i = a^j$, i.e. a is a root of unity.

(ii) Let a be a non-zero totally real integer whose conjugates all lie in the interval $[-2, 2]$. We may assume that $a \neq \pm 2$. The number $a^2/4 - 1$ is negative, and so $b = a/2 + (a^2 - 4)^{1/2}/2$ is not real. Since b is a root of $X^2 - aX + 1$, it is an algebraic integer, but obviously $\overline{|b|} = 1$, whence by (i) b is a root of unity, i.e. $b = \exp(2\pi i s)$ for a certain rational s. Since $a = 2\mathrm{Re}\, b$, we get $a = 2\cos(\pi r)$ with $r = 2s$. □

It has been observed by Schinzel and Zassenhaus [65] that for integers of a fixed degree the bound in (i) can be improved. We prove now a simple result of this type, due to Dobrowolski [78].

Theorem 2.6. *If a is an algebraic integer of degree n which is neither zero nor a root of unity, then*

$$\overline{|a|} \geq 1 + \frac{\log n}{6n^2}.$$

Proof : The assertion is trivial in case $n = 1$, so assume $n \geq 2$. Choose a rational prime p in the interval $[3n, 6n]$. Such a prime exists by Bertrand's

postulate. Let $F(X) = X^n + \sum_{j=0}^{n-1} A_j X^j \in \mathbb{Z}[X]$ be the minimal polynomial of a, and put

$$G(X) = \prod_{i=1}^{n}(X - a_i^p) = X^n + \sum_{j=0}^{n-1} B_j X^j,$$

where $a_1 = a, a_2, \ldots, a_n$ are the conjugates of a. Finally put

$$S_k = \sum_{j=1}^{n} a_j^k$$

for $k \geq 1$.

Newton's formulas imply the following equalities for $k = 1, 2, \ldots, n$:

$$\begin{aligned} S_k + A_{n-1}S_{k-1} + \cdots + A_{n-k+1}S_1 + kA_{n-k} &= 0, \\ S_{kp} + B_{n-1}S_{(k-1)p} + \cdots + B_{n-k+1}S_p + kB_{n-k} &= 0. \end{aligned} \tag{2.1}$$

Assume now that the theorem is not true for a certain a, and observe that for $k = 1, 2, \ldots, n$ we have

$$|S_{kp} - S_k| \leq 2n\overline{|a|}^{\,kp} \leq 2n\left(1 + \frac{\log n}{6n^2}\right)^{6kn} \leq 2n \exp\left(\frac{k \log n}{n}\right),$$

and since the function

$$f(t) = \frac{1}{t} \exp\left(\frac{t \log n}{n}\right)$$

has no maxima in the open interval $(1, n)$, and $f(n) = 1 \leq f(1) \leq \sqrt[3]{3} < 3/2$, we obtain

$$|S_{kp} - S_k| \leq 3kn < kp.$$

In particular, one has

$$|S_p - S_1| < p. \tag{2.2}$$

Further, for $k \geq 1$ we have the equality

$$S_k^p = (a_1^k + \cdots + a_n^k)^p = a_1^{kp} + \cdots + a_n^{kp} + pu(p, k)$$

with an integer $u(p, k)$, which is rational, being equal to $(S_k^p - S_{kp})/p$, and thus

$$S_k \equiv S_k^p \equiv S_{kp} \pmod{p} \tag{2.3}$$

holds for all $k \geq 1$.

In particular $S_1 \equiv S_p \pmod{p}$, and this together with (2.2) leads to $S_1 = S_p$. Utilizing (2.1) we get $A_{n-1} = B_{n-1}$. Assume that for $j = 1, 2, \ldots, k-1$ one has $S_{jp} = S_j$ and $A_{n-j} = B_{n-j}$. Using (2.1) and (2.3) we get $S_{kp} = S_k$, and using again (2.1) we obtain $A_{n-k} = B_{n-k}$. Finally, we see that $F(X) = G(X)$, and thus the sets $\{a_1, \ldots, a_n\}$ and $\{a_1^p, \ldots, a_n^p\}$ coincide. This however leads to a contradiction. Indeed, if K is the splitting field of F,

and $\sigma \in Gal(K/\mathbb{Q})$ carries a into a^p, then we get, denoting by N the order of σ,

$$a = \sigma^N a = a^{p^N},$$

thus a either zero or a root of a unity, contrary to our assumption. □

5. The following theorem shows that Theorem 2.5 (ii) is best possible:

Theorem 2.7. (Robinson [62]) *If I is an interval on the real axis having length > 4, then one can find in I infinitely many full sets of conjugates of algebraic integers. Moreover, for the particular intervals $[-2-\epsilon, 2+\epsilon]$ with a positive ϵ one can find such sets not containing any number of the form $2\cos(\pi r)$ with $r \in \mathbb{Q}$.*

Proof : Let c be real and $I = [c-2\lambda, c+2\lambda]$ with rational $\lambda > 1$, and define a sequence P_n of polynomials, by means of

$$P_n(X) = (2\lambda)^n T_n\left(\frac{X-c}{2\lambda}\right) \quad (n = 1, 2, \ldots),$$

where T_n is the nth Chebyshev polynomial, i.e.

$$T_n(X) = X^n + \sum_{k=1}^{[n/2]} (-1)^k \frac{n}{k4^k} \binom{n-k-1}{k-1} X^{n-2k}.$$

We shall need a few properties of P_n, which are easily deducible from the corresponding properties of Chebyshev polynomials:

(i) *One can write*

$$P_n(X) = X^n + \sum_{k=1}^{n} a_k^{(n)} X^{n-k},$$

where for fixed $k < n$ the coefficient $a_k^{(n)}$ is a polynomial in n, vanishing at zero,

(ii) *The maximal absolute value of P_n in I equals $2\lambda^n$, and is attained at $1+n$ points $u_1, \ldots, u_{n+1}$, say.*

(iii) *For $i = 1, 2, \ldots, n$ we have $P_n(u_i)P_n(u_{i+1}) < 0$.*

Choose now a rational integer M so that $\lambda^M(\lambda - 1) \geq 4$, and observe that with a suitable choice of m every coefficient $a_i^{(n)}$ $(i = 1, 2, \ldots, M)$ with n divisible by m is integral and even. In fact, with certain rational integers $\alpha_i^{(j)}$, β_k we have

$$a_k^{(n)} = \frac{\alpha_0^{(k)} n^k + \cdots + \alpha_{k-1}^{(k)} n}{\beta_k},$$

and so we may take for m the least common multiple of the numbers $2\beta_1, \ldots, 2\beta_M$.

Let $n > M$ be a rational integer divisible by m. Choose $b_{M+1}, \ldots, b_n \in [0, 4)$, such that the polynomial

$$Q_n(X) = P_n(X) + \sum_{k=1+M}^{n} b_k P_{n-k}(X) = X^n + \sum_{k=0}^{n-1} c_k X^k$$

has all its coefficients c_k integral and even with $4 \nmid c_0$ (for $k = n-M, \ldots, n-1$ this is implied by the choice of m), and note that for $n \in I$ we have

$$|P_n(x) - Q_n(x)| \leq \sum_{k=1+M}^{n} \max_{x \in I} |P_{n-k}(x)| = 8 \sum_{k=1+M}^{n} \lambda^{n-k}$$
$$= 8\frac{\lambda^{n-M} - 1}{\lambda - 1} < \frac{8\lambda^n}{\lambda^M(\lambda - 1)} \leq 2\lambda^n,$$

hence at all points u_i the polynomials P_n and Q_n attain values of coinciding signs. This shows that Q_n has exactly n zeros in I, and, since it is irreducible by Eisenstein's theorem, these zeros form a full sets of conjugates. This establishes the first part of the theorem, since we may choose n in infinitely many ways.

To prove the second part observe that the first part shows for every $\epsilon > 0$ the existence of infinitely many full sets of conjugates of integers in the interval $J_\epsilon = [-2 - \epsilon, 2 - \epsilon/2]$. Among those sets there is an infinite number of sets not containing numbers of the form $2\cos(\pi r)$ with $r \in \mathbb{Q}$. Indeed, every set containing such a number must contain $2\cos(\pi/q)$ with a suitable natural q, but this is possible only for a finite number of q's, since $2\cos(\pi/q)$ tends to 2 as q approaches infinity. It remains to observe that the interval J_ϵ is contained in $[-2 - \epsilon, 2 + \epsilon]$, □

2.2. Discriminants and Integral Bases

1. To obtain some kind of classification of algebraic number fields one introduces various functions defined on the set of all such fields. The simplest example is the degree over $\mathbb{Q}$, which, however, does not suffice, since there are infinitely many fields of the same degree. In this section we shall introduce another function, namely the *absolute discriminant* $d(K)$, which assumes non-zero integral values, and has the remarkable property, noted first by Hermite [57], of assuming the same value only for a finite number of fields. Moreover it is an invariant of isomorphisms, i.e., isomorphic fields have the same discriminants. We start with some general definitions, valid for arbitrary finite extensions of any field of zero characteristic. This slightly more

general approach will be utilized in Chap. 5, where we shall speak about completions of algebraic number fields.

Assume thus that K is a field of zero characteristic, and let L/K be a finite extension of degree n. If Ω is a fixed algebraic closure of K, then there are n distinct embeddings $F_1, \ldots, F_n$ of L into Ω, leaving K invariant. For any sequence of n elements $v_1, \ldots, v_n$ of L we define the *discriminant* $d_{L/K}(v_1, \ldots, v_n)$ by

$$d_{L/K}(v_1, \ldots, v_n) = (\det[F_i(v_j)]_{i,j})^2 .$$

Note that the discriminant does not depend on the order of the embeddings F_i or of the v_i's.

The following proposition provides an alternative definition of the discriminant:

Proposition 2.8. *If $T_{L/K}(x) = \sum_{i=1}^{n} F_i(x)$ is the trace, then for $v_1, \ldots, v_n \in L$ we have*

$$d_{L/K}(v_1, \ldots, v_n) = \det[T_{L/K}(v_i v_j)]_{i,j}.$$

Proof: It suffices to observe that with notation A^T for the transposed matrix of A we have

$$\begin{aligned} \det\left[T_{L/K}(v_i v_j)\right] &= \det\left[\sum_{k=1}^{n} F_k(v_i) F_k(v_j)\right] \\ &= \det\left([F_k(v_i)]\,[F_k(v_i)]^T\right) = d_{L/K}(v_1, \ldots, v_n). \quad \square \end{aligned}$$

If a is an arbitrary element of L, then its *discriminant* with respect to K, which we shall denote by $d_{L/K}(a)$, is defined by

$$d_{L/K}(a) = d_{L/K}(1, a, a^2, \ldots, a^{n-1}).$$

One can easily see that

$$d_{L/K}(a) = \prod_{i<j} (F_i(a) - F_j(a))^2, \tag{2.4}$$

and this shows that if a generates the extension L/K, then $d_{L/K}(a)$ coincides with the discriminant of the minimal polynomial of a over K, and thus is non-zero. If, however, a generates a proper subfield of L, then $d_{L/K}(a) = 0$.

The main properties of the discriminant are contained in the following proposition.

Proposition 2.9. *Let L/K be a finite extension and let $v_1, \ldots, v_n$ be elements of L.*

(i) *The discriminant* $d_{L/K}(v_1, \ldots, v_n)$ *lies in* K, *and if* K *is an algebraic number field, then the discriminant of a set of integers is an integer.*

(ii) *If for* $i = 1, 2, \ldots, n$ *we have* $u_i = \sum_{j=1}^{n} a_{ij} v_j$ *with* $a_{ij} \in K$, *then*

$$d_{L/K}(u_1, \ldots, u_n) = (\det [a_{ij}])^2 \, d_{L/K}(v_1, \ldots, v_n).$$

(iii) *One has* $d_{L/K}(v_1, \ldots, v_n) = 0$ *if and only if the system* $v_1, \ldots, v_n$ *is linearly dependent over* K.

(iv) *If* $L = K(a)$ *and* $P \in K[X]$ *is the minimal polynomial of* a, *then*

$$d_{L/K}(a) = (-1)^m \det[c_{ij}] = (-1)^m N_{L/K}(P'(a)),$$

where $m = n(n-1)/2$, *the elements* a_{ij} *are defined by*

$$a^j P'(a) = \sum_{i=0}^{n-1} c_{ij} a^i \quad (j = 0, 1, \ldots, n-1),$$

and P' *is the formal derivative of* P.

Proof: Part (i) results from Propositions 2.4 and 2.8, and (ii) is a consequence of the equality

$$\det [F_j(u_i)] = \det[c_{ij}] \det [F_j(v_i)] .$$

To prove (iii) note first that if the elements $v_1, \ldots, v_n$ are linearly dependent over K, then with suitable $x_1, \ldots, x_n \in K$ (not all of them vanishing) we have

$$\sum_{i=1}^{n} x_i F_j(v_i) = 0 \quad (j = 1, 2, \ldots, n),$$

and thus $d_{L/K}(v_1, \ldots, v_n) = 0$.

On the other hand, if $d_{L/K}(v_1, \ldots, v_n)$ vanishes, then the system

$$\sum_{i=1}^{n} x_i T_{L/K}(v_i v_j) = 0 \quad (j = 1, 2, \ldots, n)$$

has a non-zero solution. If the system $v_1, \ldots, v_n$ were linearly independent over K, then $u = x_1 v_1 + \cdots + x_n v_n$ would be non-zero, and $T_{L/K}(u v_i) = 0$ would hold for $i = 1, 2, \ldots, n$. Hence for all $y \in L$ we would have $T_{L/K}(uy) = 0$, but this is not possible, since taking $y = 1/u$ we obtain $n = T_{L/K}(1) = 0$.

Finally, to obtain (iv) denote by $a_1 = a, \ldots, a_n$ the conjugates of a over K, and put $b_i = P'(a_i)$, all these elements lying in a fixed algebraic closure of L. Then

$$\begin{aligned} d_{L/K}(a) &= \prod_{i<j} (a_i - a_j)^2 = (-1)^m \prod_{i=1}^{n} \prod_{j \neq i} (a_i - a_j) \\ &= (-1)^m \prod_{i=1}^{n} P'(a_i) = (-1)^m b_1 \cdots b_n = (-1)^m N_{L/K}(P'(a)). \end{aligned}$$

Moreover

$$b_1 \cdots b_n \det[a_i^j] = \det[a_i^j b_i] = \det\left[\sum_{k=1}^{n} c_{kj} a_k^i\right] = \det[c_{kj}] \det[a_j^k],$$

and since (iii) implies $\det[a_k^i] \neq 0$, we obtain

$$b_1 b_2 \cdots b_n = \det[c_{ij}],$$

and thus

$$d_{L/K}(a) = (-1)^m \det[c_{ij}],$$

as asserted. □

2. Now we leave the abstract situation, and return to algebraic number fields, to which the concepts developed in the preceding subsection apply. We shall use them for the definition of the field discriminant. Let K be an algebraic number field of degree n. A system $\omega_1, \ldots, \omega_n$ of integers of K, which is linearly independent over the rationals and generates R_K as a $\mathbb{Z}$-module, is called an *integral basis* of K. Note that the existence of a system $\omega_1, \ldots \omega_n$ of elements of R_L, which is linearly independent over K and generates R_L as a R_K-module is equivalent to the fact that R_L is a free R_K-module. We shall see that this is the case when $K = \mathbb{Q}$, but may fail in the general case. The question, when this happens will be answered in Chap. 7 (see Corollary 1 to Theorem 7.42).

Theorem 2.10. *Every algebraic number field has an integral basis, i.e., for every finite extension $K/\mathbb{Q}$, R_K is a free $\mathbb{Z}$-module.*

Proof: Let $a \in R_K$ be a generator of the extension $K/\mathbb{Q}$. Lemma 1.21 implies $d_{K/\mathbb{Q}}(a) R_K \subset \mathbb{Z}[a]$, whence $R_K \subset d_{K/\mathbb{Q}}^{-1}(a)\mathbb{Z}[a]$.

Since $\mathbb{Z}[a]$ is a free $\mathbb{Z}$-module with finitely many generators a^i ($i = 0, 1, \ldots, n-1$, $n = [K : \mathbb{Q}]$), it is Noetherian by Proposition 1.2, and hence $d_{K/\mathbb{Q}}^{-1}(a)\mathbb{Z}[a]$ is also Noetherian. Thus R_K is a finitely generated torsion-free $\mathbb{Z}$-module, and Theorem 1.32 implies that R_K is isomorphic as a $\mathbb{Z}$-module to $\mathbb{Z}^d$ for a certain $0 \leq d \leq n$, because $\mathbb{Z}$ is a principal ideal domain. However R_K spans an n-dimensional $\mathbb{Q}$-space, and so $d = n$. □

We give also an alternative proof of the last theorem, which permits the construction of an integral basis of a special form, needed in the sequel.

Proposition 2.11. *If $[K : \mathbb{Q}] = n$ and the numbers $a_1, \ldots, a_n$ of R_K are linearly independent over $\mathbb{Q}$, then there exists an integral basis $\omega_1, \ldots, \omega_n$ of K such that for $j = 1, 2, \ldots, n$ one has, with suitable $c_{ij} \in \mathbb{Z}$,*

$$a_j = c_{j1}\omega_1 + \cdots + c_{jj}\omega_j.$$

Proof : Put $d = d_{K/\mathbb{Q}}(a_1, \ldots, a_n)$ and for $i = 1, 2, \ldots, n$ denote by d_{ii} the least positive integer such that with suitably chosen $d_{ik} \in \mathbb{Z}$ $(1 \leq k \leq i-1)$ one has

$$\omega_i = \frac{1}{d} \sum_{j=1}^{i} d_{ij} a_j \in R_K.$$

The numbers $\omega_1, \ldots, \omega_n$ are linearly independent over $\mathbb{Q}$, since their discriminant D satisfies

$$D = (d^{-n} \det[d_{ij}])^2 d,$$

and

$$\det[d_{ij}] = d_{11} d_{22} \cdots d_{nn} \neq 0$$

by Proposition 2.9.

Observe now that if $c \in R_K$ can be written in the form

$$c = \frac{c_1 a_1 + \cdots + c_j a_j}{d},$$

with a certain j and $c_i \in \mathbb{Z}$, then $d_{jj} | c_j$. Indeed, if $c_j = s d_{jj} + r$ with $r, s \in \mathbb{Z}$ and $0 < r < d_{jj}$, then $c - s\omega_j \in R_K$, and

$$c - s\omega_j = \frac{(c_1 - s d_{j1}) a_1 + \cdots + r a_j}{d},$$

contrary to the choice of d_{jj}. Let M_0 be the $\mathbb{Z}$-module generated by $\omega_1, \ldots, \omega_n$. We shall prove by induction in j that M_0 contains every element of R_K of the form $(x_1 a_1 + \cdots + x_j a_j)/d$ $(x_i \in \mathbb{Z})$. For $j = 1$ the assertion is obvious, so assume it holds for all indices $< j$, and consider $y = (x_1 a_1 + \cdots + x_j a_j)/d \in R_K$, where $x_i \in \mathbb{Z}$. Then, with a suitable $A \in \mathbb{Z}$, we have $x_j = A d_{jj}$, thus $y - A\omega_j \in R_K$, and, in view of $A\omega_j \in M_0$, it suffices to apply the inductional assumption.

For $j = n$ this gives $M_0 = R_K$, because by Lemma 1.21 we have $R_K \subset (a_1 \mathbb{Z} + \cdots + a_n \mathbb{Z})/d$, and the proposition follows. □

Examples of integral bases will be given in the last part of this section.

3. In this subsection we shall define the discriminant of any $\mathbb{Z}$-module of finite index in R_K, a special case of which will be the discriminant of the field K. The following proposition shows that all free bases of a free $\mathbb{Z}$-module have the same discriminant.

Proposition 2.12. *If M is a free $\mathbb{Z}$-module with n free generators $a_1, \ldots, a_n$, and $b_1, \ldots, b_n$ is another set of its free generators, then for some matrix $[c_{ij}]$ with elements from $\mathbb{Z}$ and determinant ± 1 one has*

$$b_i = \sum_{j=1}^{n} c_{ij} a_j. \tag{2.5}$$

Conversely, if $a_1, \ldots, a_n$ *generate freely a* $\mathbb{Z}$*-module* M*, and the elements* $b_1, \ldots, b_n$ *of* M *are related to the* a_i*'s through* (2.5) *with* $\det[c_{ij}] = \pm 1$*, then they also form a free basis of* M*.*

Proof : If the a_i's and b_i's are free generators, then the matrix $[c_{ij}]$ has an inverse with elements in $\mathbb{Z}$, and so its determinant equals 1 or -1. The second part of the proposition results from the observation that under the given conditions the matrix $[c_{ij}]$ has an inverse with elements in $\mathbb{Z}$. □

Corollary. *If* $[K : \mathbb{Q}] = n$ *and* $M \subset R_K$ *is a free* $\mathbb{Z}$*-module with* n *free generators, then the discriminant of a basis of* M *does not depend on the choice of that basis.*

Proof : This follows from the proposition just proved and Proposition 2.9 (ii). □

Proposition 2.12 suggests the following definition: if $M \subset R_K$ is a free $\mathbb{Z}$-module with $n = [K : \mathbb{Q}]$ free generators, then the *discriminant* $d_{K/\mathbb{Q}}(M)$ of M is defined as the discriminant of any basis of M. In particular, if $M = R_K$, then this discriminant is called the *discriminant of the field* K, and is denoted by $d(K)$. It is the discriminant of any integral basis of K. Proposition 2.9 (ii) shows that $|d(K)|$ equals the greatest common divisor of all $d_{K/\mathbb{Q}}(v_1, \ldots, v_n)$ with $v_1, \ldots, v_n \in R_K$. The next proposition makes this fact more precise:

Proposition 2.13. *If* $a_1, \ldots, a_n$ *are linearly independent over* $\mathbb{Q}$*, then*

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = m^2 d(K),$$

where m *is the index in* R_K *of the* $\mathbb{Z}$*-module* M *generated by the* a_i*'s.*

Proof : Let $\omega_1, \ldots, \omega_n$ be an integral basis of K, and choose the numbers $b_1, \ldots, b_n \in M$ in such a way that

$$b_i = \sum_{k=1}^{i} c_{ik}\omega_k \quad (c_{ik} \in \mathbb{Z}, i = 1, \ldots, n),$$

where c_{ii} is positive and as small as possible. As in the proof of Proposition 2.11 we see that the b_i's form a set of free generators for M, and that $\sum_{k=1}^{i} t_k\omega_k$ (with $t_k \in \mathbb{Z}$) can lie in M only if c_{ii} divides t_i. This shows that the numbers

$$\sum_{k=1}^{n} \alpha_k\omega_k \quad (0 \leq \alpha_k < c_{kk}, k = 1, \ldots, n)$$

are pairwise incongruent mod M, and obviously there are $c_{11} \cdots c_{nn}$ of them. We shall show that they represent all residue classes mod M. Let

$$\xi = \sum_{k=1}^{n} \lambda_k \omega_k \quad (\lambda_k \in \mathbb{Z})$$

be an arbitrary element of R_K, denote by μ_n the least non-negative residue of $\lambda_n \bmod c_{nn}$, and put $A_n = (\lambda_n - \mu_n)/c_{nn}$. Then

$$\xi = A_n b_n + \mu_n \omega_n + \sum_{k=1}^{n-1} (\lambda_k - A_n c_{nk}) \omega_k.$$

If by μ_{n-1} we denote the least non-negative residue of

$$\lambda_{n-1} - A_n c_{n,n-1} \bmod c_{n-1,n-1},$$

and put

$$A_{n-1} = (\lambda_{n-1} - A_n c_{n,n-1} - \mu_{n-1})/c_{n-1,n-1},$$

then

$$\begin{aligned} \xi =& A_n b_n + A_{n-1} b_{n-1} + \mu_n \omega_n + \mu_{n-1} \omega_{n-1} \\ &+ \sum_{k=1}^{n-2} (\lambda_k - A_n c_{n,k} - A_{n-1} c_{n-1,k}) \omega_k. \end{aligned}$$

Continuing this procedure, we finally obtain an equality of the form

$$\xi = \sum_{k=1}^{n} A_k b_k + \sum_{k=1}^{n} \mu_k \omega_k \quad (0 \le \mu_k < c_{kk}; \mu_k, A_k \in \mathbb{Z}),$$

and so

$$\xi \equiv \sum_{k=1}^{n} \mu_k \omega_k \pmod{M},$$

as required. Now it suffices to observe that

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = d_{K/\mathbb{Q}}(b_1, \ldots, b_n) = (c_{11} \cdots c_{nn})^2 d(K),$$

by Proposition 2.9 (ii). □

Corollary. *If $a \in K$ is non-zero and $I = aR_K$, then $N(I) = |N_{K/\mathbb{Q}}(a)|$.*

Proof : Since both sides of the asserted equality are multiplicative in a, we may assume that $a \in R_K$. Let $\omega_1, \ldots, \omega_n$ be an integral basis of K. Then aR_K is the $\mathbb{Z}$-module generated by $a\omega_1, \ldots, a\omega_n$, hence the proposition implies

$$N(I)^2 = d_{K/\mathbb{Q}}(a\omega_1, \ldots, a\omega_n)/d(K),$$

but obviously $d_{K/\mathbb{Q}}(a\omega_1, \ldots, a\omega_n) = N_{K/\mathbb{Q}}^2(a) d(K)$, and our assertion follows. □

In the case when M is the $\mathbb{Z}$-module generated by $1, a, \ldots, a^{n-1}$, where a is an element of R_K of degree $n = [K : \mathbb{Q}]$, i.e., M is the subring $\mathbb{Z}[a]$ of R_K, generated by a, then the index of M in R_K is called the *index of a in R_K*, or, which is slightly incorrect, the *index of a in K*.

4. Not every non-zero rational integer is a discriminant of an algebraic number field. This is implied by the following result of L.Stickelberger [97]:

Theorem 2.14. *The discriminant $d(K)$ of a field K is congruent either to* 0 *or to* 1 mod 4.

Proof : Let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be an integral basis of K, and let $\omega_i^{(j)}$ $(i, j = 1, 2, \ldots, n)$ be all the conjugates of the ω_i's. For a permutation $P = (\mu_1, \ldots, \mu_n)$ of the set $\{1, 2, \ldots, n\}$ put $S_P = \omega_1^{(\mu_1)} \cdots \omega_n^{(\mu_n)}$. Then

$$\det[\omega_i^{(j)}] = \sum_{P \text{ even}} S_P - \sum_{P \text{ odd}} S_P = A - B.$$

If L is the field generated by all conjugates of the ω_i's, then $A, B \in R_L$, and moreover the numbers $A + B$ and AB are rational integers, since they are invariant under the automorphisms of L. Now

$$d(K) = (A - B)^2 = (A + B)^2 - 4AB \equiv (A + B)^2 \pmod 4,$$

and so $d(K) \equiv 0, 1 \pmod 4$. □

Our next proposition, due to A.Brill [77], determines the sign of the discriminant.

Proposition 2.15. *If $[r_1, r_2]$ is the signature of K, then* $\operatorname{sgn} d(K) = (-1)^{r_2}$.

Proof : Once again let $\omega_1, \ldots, \omega_n$ be an integral basis of K, and $\omega_i^{(j)}$ the conjugates of ω_i's. Write $\det[\omega_i^{(j)}] = d_1 + id_2$ with $d_1, d_2 \in \mathbb{R}$. Since the change of i into $-i$ in this determinant is equivalent to the interchange of r_2 pairs of rows, we have $d_1 - id_2 = (-1)^{r_2}(d_1 + id_2)$. If r_2 is even, this implies $d_2 = 0$, hence $d(K) = d_1^2 > 0$, and if r_2 is odd, then $d_1 = 0$ and $d(K) = (id_2)^2 = -d_2^2 < 0$. □

We conclude this subsection with a result of L.Kronecker, which will be strengthened later (see Corollary 1 to Proposition 4.15), however we prove it here, as it will be of some use in the sequel.

Proposition 2.16. *If $\mathbb{Q} \subset K \subset L$, then $d(K)$ divides $d(L)$.*

Proof : Let $[K : \mathbb{Q}] = m$, $[L : K] = n$. Let $a_1, \ldots, a_m$ be an integral basis of K, and choose $a_{m+1}, \ldots, a_{mn} \in R_L$ so, that the resulting set $a_1, \ldots, a_{mn}$ is $\mathbb{Q}$-independent. Proposition 2.11 implies the existence of an integral basis $\omega_1, \ldots, \omega_{mn}$ of L such that

$$a_j = \sum_{k=1}^{j} c_{jk}\omega_k \quad (j = 1, \ldots, mn)$$

holds with $c_{jk} \in \mathbb{Z}$. The elements $\omega_1, \ldots, \omega_m$ lie in K, and the $\mathbb{Z}$-module generated by them contains an integral basis of K, hence they form an integral basis of K. As usual, denote by $\omega_j^{(i)}$ the conjugates of the ω_j's, and let $F_1, \ldots, F_m$ be embeddings of L into $\mathbb{C}$ satisfying $\omega_j^{(i)} = F_i(\omega_j)$ for $i, j = 1, \ldots, m$. Denote the remaining embeddings of L in $\mathbb{C}$ by $F_{m+1}, \ldots, F_{mn}$, and assume that $F_i(\omega_j) = \omega_j^{(i)}$ holds for all j and $i = m+1, \ldots, mn$. Assume moreover that for $x \in K$ and $i \equiv k \pmod{m}$ one has $F_i(x) = F_k(x)$. Consequently we get

$$\begin{aligned}
d(L) &= \left(\det[\omega_j^{(i)}]\right)^2 \\
&= \begin{vmatrix}
\omega_1^{(1)} & \ldots & \omega_1^{(m)} & \omega_1^{(1)} & \ldots & \omega_1^{(m)} & \ldots & \omega_1^{(1)} & \ldots & \omega_1^{(m)} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_m^{(1)} & \ldots & \omega_m^{(m)} & \omega_m^{(1)} & \ldots & \omega_m^{(m)} & \ldots & \omega_m^{(1)} & \ldots & \omega_m^{(m)} \\
\omega_{m+1}^{(1)} & \ldots & \omega_{m+1}^{(m)} & \omega_{m+1}^{(m+1)} & \ldots & \ldots & \ldots & \ldots & \ldots & \omega_{m+1}^{(mn)} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_{mn}^{(1)} & \ldots & \omega_{mn}^{(m)} & \omega_{mn}^{(m+1)} & \ldots & \ldots & \ldots & \ldots & \ldots & \omega_{mn}^{(mn)}
\end{vmatrix}^2 \\
&= \begin{vmatrix}
\omega_1^{(1)} & \ldots & \omega_1^{(m)} & 0 & \ldots & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_m^{(1)} & \ldots & \omega_m^{(m)} & 0 & \ldots & \ldots & 0 \\
\omega_{m+1}^{(1)} & \ldots & \omega_{m+1}^{(m)} & \omega_{m+1}^{(m+1)} - \omega_{m+1}^{(1)} & \ldots & \ldots & \omega_{m+1}^{(mn)} - \omega_{m+1}^{(m)} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_{mn}^{(1)} & \ldots & \omega_{mn}^{(m)} & \omega_{mn}^{(m+1)} - \omega_{mn}^{(1)} & \ldots & \ldots & \omega_{mn}^{(mn)} - \omega_{mn}^{(m)}
\end{vmatrix}^2 \\
&= d(K)a,
\end{aligned}$$

where a is an algebraic integer. However $a = d(L)/d(K)$ is rational, and thus it is a rational integer. □

5. Now we shall compute some examples of integral bases and discriminants. We start with a lemma which is sometimes useful in determining the discriminant.

Lemma 2.17. *Let a be an algebraic integer, and let $K = \mathbb{Q}(a)$ be the field generated by it. If the minimal polynomial over $\mathbb{Q}$ of a is Eisensteinian with respect to the prime p, i.e., it has the form $X^n + a_{n-1}X^{n-1} + \cdots + a_0$, with $a_0, \ldots, a_{n-1}$ divisible by p and $p^2 \nmid a_0$, then the index of a in K is not divisible by p.*

Proof : Our assumptions imply that a^n/p is an integer, and, moreover, p^2 does not divide $N_{K/\mathbb{Q}}(a)$. Assume that p divides the index of a. Then there exists an integer $\xi \in R_K$ of the form

$$\xi = (b_0 + b_1 a + \cdots + b_{n-1}a^{n-1})/p \quad (b_i \in \mathbb{Z}),$$

not all of the b_i's divisible by p. Let j be the minimal index with $p \nmid b_j$. Then the number

$$\begin{aligned}\eta &= (b_j a^j + \cdots + b_{n-1}a^{n-1})/p \\ &= \xi - (b_0 + b_1 a + \cdots + b_{j-1}a^{j-1})/p\end{aligned}$$

is an integer, and so is also

$$\zeta = b_j a^{n-1}/p = \eta a^{n-j-1} - a^n(b_{j+1} + b_{j+2}a + \cdots + b_{n-1}a^{n-j-2})/p.$$

This implies

$$p^n N_{K/\mathbb{Q}}(\zeta) = N_{K/\mathbb{Q}}(p\zeta) = N_{K/\mathbb{Q}}(b_j a^{n-1}) = b_j^n N_{K/\mathbb{Q}}(a)^{n-1},$$

hence p has to divide b_j, contrary to the choice of j. □

With the use of this lemma it is sometimes possible to find the exact power of a prime p dividing the discriminant of a field K. This happens when we have an integer a generating K, and satisfying the conditions of the lemma, because then, by Proposition 2.13, $d_{K/\mathbb{Q}}(a)$ and $d(K)$ are divisible by the same power of p.

Another fact will be used quite often, namely the equality $d_{K/\mathbb{Q}}(a) = d_{K/\mathbb{Q}}(a+n)$ for $n \in \mathbb{Z}$, which follows directly from (2.4).

Let us now give some examples. We begin with quadratic fields.

Theorem 2.18. *Let D be a square-free rational integer, and let $K = \mathbb{Q}(\sqrt{D})$. Then*

$$d(K) = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{otherwise,} \end{cases}$$

and an integral basis of K is formed by $1, \omega$, where

$$\omega = \begin{cases} (1+\sqrt{D})/2 & \text{if } D \equiv 1 \pmod 4, \\ \sqrt{D} & \text{otherwise.} \end{cases}$$

(It is irrelevant which of the two possible square roots of D we take here; however, it is convenient to assume that for positive D the number $\sqrt{D}$ is assumed to be positive, whereas for negative D the square root lies on the upper imaginary half-axis.)

Proof : The polynomial $X^2 - D$ is Eisensteinian for any prime dividing D, and since its discriminant equals $4D$, we obtain for even D the equality

$d(K) = 4D$ by Lemma 2.17 and Proposition 2.13. If $D \equiv 3 \pmod 4$, then the polynomial $(X+1)^2 - D$ is Eisensteinian for $p = 2$, and since its root equals $\sqrt{D} - 1$, and its discriminant is $4D$, we get again $d(K) = 4D$. Since in both cases we have $d_{K/\mathbb{Q}}(1, \sqrt{D}) = 4D$, the numbers 1 and $\sqrt{D}$ form an integral basis.

If $D \equiv 1 \pmod 4$, then ω is integral, being the root of $X^2 - X + (1-D)/4$. Moreover its discriminant equals D, which is square-free, thus by Proposition 2.13 we get $d(K) = D$, and $1, \omega$ form an integral basis. □

Now let K be a pure cubic field, i.e., $K = \mathbb{Q}(\sqrt[3]{m})$ with $m \in \mathbb{Z}$, not divisible by a cube of a prime. We can write $m = ab^2 > 0$ with ab square-free (thus $(a, b) = 1$). Moreover, in the case $3|m$ we may assume $3|a$, $3 \nmid b$, because the fields generated by $\sqrt[3]{ab^2}$ and $\sqrt[3]{a^2b}$ coincide.

Theorem 2.19. *If $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt[3]{m}$ with $m = ab^2$ as given above, then one distinguishes between three cases:*

(i) $m \not\equiv \pm 1 \pmod 9$. *Here $d(K) = -27(ab)^2$, and the numbers $1, \theta, \theta^2/b$ form an integral basis,*

(ii) $m \equiv 1 \pmod 9$. *In this case $d(K) = -3(ab)^2$, and the numbers $\theta, \theta^2/b, (1 + \theta + \theta^2)/3$ form an integral basis,*

(iii) $m \equiv -1 \pmod 9$. *Here $d(K) = -3(ab)^2$, and an integral basis is formed by $\theta, \theta^2/b, (1 - \theta + \theta^2)/3$.*

Proof : Using Proposition 2.9 (iv) we get $d_{K/\mathbb{Q}}(\theta) = -3^3m^2$. The minimal polynomial for θ, $X^3 - m$, is Eisensteinian for every prime divisor of a. If $3|a$, then we get $3^3a^2|d(K)$, and if $3 \nmid a$, then $3a^2|d(K)$. The number $\vartheta = \theta^2/b$ is a root of $X^3 - a^2b$, which is Eisensteinian for every prime dividing b, and therefore $b^2|d(K)$. Finally we obtain $d(K) = -3^N(ab)^2$, where N is equal to 3 if $3|m$, and is equal to either 1 or 3 otherwise.

If $m \not\equiv \pm 1 \pmod 9$, then $m^3 \not\equiv m \pmod 9$, thus $(X+m)^3 - m$ is Eisensteinian for $p = 3$, and the discriminant of its root $\theta - m$ equals -3^3m^2. Hence Lemma 2.17 implies $d(K) = -3^3(ab)^2$.

If $m \equiv 1 \pmod 9$, then the number $\psi = (1 + \theta + \theta^2)/3$ is an integer, since it is a root of the polynomial

$$X^3 - X^2 + \frac{1-m}{3}X - \frac{(m-1)^2}{27}.$$

This shows that the index of θ is divisible by 3, and Proposition 2.13 leads to $d(K) = -3(ab)^2$.

A similar argument applies to the case $m \equiv -1 \pmod 9$, in which case we have to consider $(1 - \theta + \theta^2)/3$ in place of ψ.

The assertion concerning integral bases can be now verified directly by calculating the discriminants of the relevant sets, and noting that they are equal to the field discriminant. □

As our last example we consider cyclotomic fields $K = \mathbb{Q}(\zeta_n)$ in the case when n is a prime power. The general case will be treated in Chap. 4 (see Theorem 4.27 (ii)).

Theorem 2.20. *Let p be a prime, $n \geq 1$, $q = p^n > 2$, and let ζ_q be a primitive q-th root of unity. Put $K = \mathbb{Q}(\zeta_q)$. The extension $K/\mathbb{Q}$ is normal of degree $N = \varphi(q) = p^{n-1}(p-1)$, and its Galois group is isomorphic to the multiplicative group $G(q)$ of residue classes* mod q, *not divisible by p. The numbers $1, \zeta_q, \ldots, \zeta_q^{N-1}$ form an integral basis of K, and*

$$d(K) = \begin{cases} 2^M & \text{if } p = 2, n \geq 2, \\ -4 & \text{if } p = n = 2, \\ \epsilon(p^n)p^M & \text{if } p > 2, \end{cases}$$

where $M = n\varphi(p^n) - p^{n-1}$, and

$$\epsilon(p^n) = \begin{cases} 1 & \text{if } p \equiv 1 \,(\text{mod } 4), \\ -1 & \text{if } p \equiv 3 \,(\text{mod } 4). \end{cases}$$

Proof : Since every q-th root of unity is a power of ζ_q, the normality of the extension follows. To show that $N = \varphi(q)$ it suffices to establish the irreducibility of the polynomial

$$W(X) = (X^{p^n} - 1)/(X^{p^{n-1}} - 1)$$

over the rationals, as $W(\zeta_q) = 0$. Consider $F(X) = W(X+1)$. Easy induction shows that for $j = 1, 2, \ldots$ we can write

$$(1+X)^{jp^{n-1}} \equiv (1 + X^{p^{n-1}})^j \pmod{p},$$

and therefore

$$F(X) \equiv \sum_{j=0}^{p-1} \left(1 + X^{p^{n-1}}\right)^j \equiv \sum_{j=1}^{p} \binom{p}{j} X^{p^{n-1}(j-1)} \equiv X^{p^{n-1}(p-1)} \pmod{p}.$$

Since $F(0) = W(1) = p$ we see that F is Eisensteinian with respect to p, hence is irreducible over $\mathbb{Q}$, and the same holds for W. This proves our assertion about the degree of K. To determine the Galois group observe that the irreducibility of W implies that all primitive roots of unity of order q are conjugated, and so for $1 \leq a < q$, $p \nmid a$ the map $\zeta_q \mapsto \zeta_q^a$ extends to an automorphism $g_a \in Gal(K/\mathbb{Q})$. One sees easily that the associated map $G(q) \longrightarrow Gal(K/\mathbb{Q})$ is an isomorphism.

To find the discriminant we use Proposition 2.9 (iv), which gives

$$d_{K/\mathbb{Q}}(\zeta_q) = \pm N_{K/\mathbb{Q}}(W'(\zeta_q)).$$

Since

$$W'(\zeta_q) = \frac{p^n}{\zeta_q(\zeta_q^{p^{n-1}} - 1)},$$

$N_{K/\mathbb{Q}}(\zeta_q) = 1$, and $\zeta_q^{p^{n-1}} = \zeta_p$ is a primitive p-th root of unity, we get

$$d_{K/Q}(\zeta_q) = \pm\frac{p^{n\varphi(q)}}{N_{K/\mathbb{Q}}(\zeta_p - 1)}.$$

If $K_0 = \mathbb{Q}(\zeta_p)$, then, using Proposition 2.4 (iii), we get

$$\begin{aligned} N_{K/\mathbb{Q}}(\zeta_p - 1) &= N_{K_0/\mathbb{Q}}\left(N_{K/K_0}(\zeta_p - 1)\right) \\ &= N_{K_0/\mathbb{Q}}\left((\zeta_p - 1)^{\varphi(q)/(p-1)}\right) \\ &= N_{K_0/\mathbb{Q}}(\zeta_p - 1)^{p^{n-1}}. \end{aligned}$$

The formula for $d(K)$ follows now from the equality

$$N_{K_0/\mathbb{Q}}(\zeta_p - 1) = \prod_{j=1}^{p-1}(\zeta_p^j - 1) = (-1)^{p-1}\prod_{j=1}^{p-1}(1 - \zeta_p^j) = (-1)^{p-1}p,$$

and its sign $\epsilon(q)$ is determined by Proposition 2.15.

Finally, observe that $d_{K/\mathbb{Q}}(\zeta_q) = d_{K/\mathbb{Q}}(\zeta_q - 1)$, and $\zeta_q - 1$ is the root of W, which, as we have seen, is p-Eisensteinian. Therefore $d_{K/\mathbb{Q}}(\zeta_q) = d(K)$, and the powers of ζ_q form an integral basis. □

6. The results of the preceding subsection show that certain fields K have integral bases, consisting of powers of an element $a \in R_K$, in which case $R_K = \mathbb{Z}[a]$. Such fields are called *monogenic*, and such a basis is called a *power integral basis*. A necessary and sufficient for a field to be monogenic is the existence of an element $a \in R_K$ having index 1, i.e., satisfying $d(K) = d_{K/\mathbb{Q}}(a)$. It has been discovered by Dedekind [78] that there exist fields K in which the greatest common divisor of the indices of elements of R_K is greater that 1. Obviously such field cannot have a power basis. Here is Dedekind's example: Let $K = \mathbb{Q}(a)$, where a is any root of the irreducible polynomial $X^3 - X^2 - 2X - 8$. The number $b = (a^2 + a)/2$ is a root of $X^3 - 3X^2 - 10X - 8$, hence is integral, and one has $d_{K/\mathbb{Q}}(1, a, b) = -503$. Since 503 is a prime number, this shows that $1, a, b$ is an integral basis of K and $d(K) = -503$. We shall now prove that for all $x \in R_K$ one has $2|d_{K/\mathbb{Q}}(x)$, and so every integer of K has an even index.

Write $x = A + Ba + Cb$ with $A, B, C \in \mathbb{Z}$. Since $b^2 = 6 + 2a + 3b$, $a^2 = 2b - a$ and $ab = 2b + 4$, we have $x^2 = (A^2 + 6C^2 + 8BC) + (2C^2 - B^2 + 2AB)a + (2B^2 + 3C^2 + 2AC + 4BC)b$, and hence

$$d_{K/\mathbb{Q}}(x) \equiv \begin{vmatrix} 1 & 0 & 0 \\ A & B & C \\ A^2 & -B^2 & 3C^2 \end{vmatrix} \equiv (BC)^2(B + C) \equiv 0 \pmod 2.$$

Rational integers > 1 which divide all indices of integers of K are traditionally called *common non-essential discriminantial divisors*. We shall consider them more closely in Chap. 4 (see Theorem 4.34 and Proposition 4.36).

Even if K has no common non-essential discriminantial divisors, a power basis need not exist. To give an example we prove first a result of Hensel [94b].

Proposition 2.21. *To every field K of degree n over $\mathbb{Q}$ there corresponds a form F of degree $n(n-1)/2$ in $n-1$ variables with coefficients from $\mathbb{Z}$ such that the set*

$$\{|F(a_1, \ldots, a_{n-1})| : a_1, \ldots, a_{n-1} \in \mathbb{Z}\} \setminus \{0\}$$

coincides with the set of indices of integers of K.

Proof : Proposition 2.11 implies the existence of an integral basis of K of the form $\omega_1 = 1, \omega_2, \ldots, \omega_n$. If now $x = \sum_{i=1}^{n} A_i\omega_i \in R_K$ $(A_i \in \mathbb{Z})$, then the index of x equals the index of $x - A_1\omega_1 = x - A_1$. To calculate it explicitly observe that for $j = 1, 2, \ldots, n$ we have

$$(x - A_1)^j = \sum_{k=1}^{n} f_k^{(j)}(A_2, \ldots, A_n)\omega_k,$$

where the $f_k^{(j)}$'s are forms of degree j in $n-1$ variables, with coefficients in $\mathbb{Z}$. Propositions 2.9 and 2.13 imply that $|\det\left[f_k^{(j)}\right]|$ equals the index of x if x generates K, and equals 0 otherwise. Putting $F(X_1, \ldots, X_{n-1}) = \det\left[f_k^{(j)}(X_1, \ldots, X_{n-1})\right]$ we obtain the assertion. □

The form occurring in this proposition is called the *index form*. Of course, it depends on the choice of the integral basis. A field has a power basis if the index form represents 1 or -1. To give the promised example of a non-monogenic field without common non-essential discriminantial divisors consider $K = \mathbb{Q}(\sqrt[3]{m})$, with $m = ab^2$, ab square-free, $3 \nmid m$ and m not congruent to ± 1 mod 9. By Theorem 2.19 the numbers $1, \sqrt[3]{m}, \sqrt[3]{m^2}/b$ form an integral basis of K, and a short computation shows that the index form F equals $bX_1^3 - aX_2^3$. Since $(a, b) = 1$ and F represents both a and b, there cannot be any common divisor of the indices of integers of K. Now putting $a = 7$, $b = 5$ we obtain a non-monogenic field, since the form $5X_1^3 - 7X_2^3$ does not represent ± 1, the congruence $5X^3 \equiv \pm 1 \pmod 7$ being insolvable.

2.3. Applications of Minkowski's Convex Body Theorem

1. In this section we shall present some results concerning evaluations of field discriminants, obtained by means of the convex body theorem of Minkowski. We start with a classical lower bound for $d(K)$, proved first by Minkowski [91b]:

Theorem 2.22. *If the field K of degree $n \geq 1$ has the signature $[r_1, r_2]$, then*

$$|d(K)| \geq \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2.$$

We shall utilize a lemma, of which our theorem is an easy consequence:

Lemma 2.23. *Let K be a field of degree n and signature $[r_1, r_2]$. If M is a $\mathbb{Z}$-module of finite index m in R_K, then there is a non-zero $a \in M$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq m \left(\frac{4}{\pi}\right)^{r_2} \left(\frac{n!}{n^n}\right) \sqrt{|d(K)|}.$$

Proof: Let Ψ be the homomorphism of the additive group of R_K into the real n-space, occurring in Lemma 2.1, and put $\Lambda = \Psi(M)$. Since Ψ is injective we see that Λ is a lattice, and one checks without pain that its discriminant $d(\Lambda)$ equals $m\sqrt{|d(K)|}2^{-r_2}$.

Now choose $t > 0$, and let $X_t \subset \mathbb{R}^n$ be defined by

$$X_t = \{[x_1, \ldots, x_{r_1}, y_{r_1+1}, z_{r_1+1}, \ldots, y_k, z_k] : \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{k} \sqrt{y_j^2 + z_j^2} < t\},$$

where $k = r_1 + r_2$. The set X_t is convex, bounded and symmetrical about the origin. We prove now that its volume equals

$$V(X_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}. \tag{2.6}$$

In the case of $r_1 + r_2 = 1$ this is evident. Assume now that (2.6) holds for $r_1 = A$ and $r_2 = B$. Then for $r_1 = A + 1$, $r_2 = B$ we have

$$V(X_t) = \frac{2^{A-B}\pi^B}{(A+2B)!} \int_{-t}^{t} (t - |x|)^{A+2B} dx = \frac{2^{A+1-B}\pi^B}{(A+1+2B)!} t^{A+2B+1},$$

and, similarly, for $r_1 = A$, $r_2 = B + 1$ we get

$$V(X_t) = \frac{2^{A-B}\pi^B}{(A+2B)!} \iint_{y^2+z^2 \le t^2/4} (t - 2\sqrt{y^2+z^2})^{A+2B} dydz$$
$$= \frac{2^{A-1-B}\pi^{1+B}}{(A+2+2B)!} t^{A+2B+2}.$$

For any given $\epsilon > 0$ determine $t = t(\epsilon)$ from the equality

$$t^n = m \left(\frac{4}{\pi}\right)^{r_2} n! \sqrt{|d(K)|} + \epsilon.$$

Then $V(X_t)$ exceeds $2^n d(\Lambda)$, and so the convex body theorem implies the existence of $a = a(\epsilon) \neq 0$ in M such that the point $\Psi(a)$ lies in X_t. If $\Psi(a) = [x_1, \ldots, z_k]$, then

$$\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{k} \sqrt{y_j^2 + z_j^2} < t.$$

The inequality between the arithmetic and geometric means implies now

$$|N_{K/\mathbb{Q}}(a)|^{1/n} = \left(\prod_{i=1}^{r_1} |x_i| \prod_{j=1+r_1}^{k} (y_j^2 + z_j^2) \right)^{1/n} \le \frac{t}{n},$$

whence

$$|N_{K/\mathbb{Q}}(a)| \le \frac{t^n}{n^n} \le m \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d(K)|} + \frac{\epsilon}{n^n}. \tag{2.7}$$

Observe finally that for $\epsilon \in (0,1)$ we have only finitely many number of possibilities for $a(\epsilon)$, and so there must exist an $a_0 \in M$, satisfying the last inequality for all $\epsilon > 0$, and this establishes the lemma. □

Proof of Theorem 2.22: Apply Lemma 2.23 with $M = R_K$, $m = 1$, and observe that for non-zero $a \in R_K$ we have $|N_{K/\mathbb{Q}}(a)| \ge 1$. □

Let us point out three consequences:

Corollary 1. *If K is a field of degree n, then*

$$|d(K)| \ge \left(\frac{11}{12}\right)^2 \left(\frac{\pi e^2}{4}\right)^n \frac{1}{2\pi n}. \tag{2.8}$$

Proof : Stirling's formula gives $n^n/n! = \exp(n - \vartheta/12n)(2\pi n)^{-1/2}$ with a certain $0 < \vartheta < 1$, and since $\exp(1/12) \le 12/11$ and $n \ge 1$, the stated evaluation results. □

Corollary 2. *If $K \neq \mathbb{Q}$ is an algebraic number field, then $|d(K)| > 1$.*

Proof : It suffices to observe that the function

$$f(t) = t\log(\pi e^2/4) - \log t - \log(2\pi) - \log(144/121)$$

is positive at $t = 2$ and increases in $[2, \infty]$, and apply Corollary 1. □

Denote by $M(r_1, r_2)$ the smallest absolute value of the discriminant of a field with signature $[r_1, r_2]$.

Corollary 3. *One has* $\lim_{r_1+r_2\to\infty} M(r_1, r_2) = \infty$. □

2. Now we can prove the result of Hermite. mentioned at the beginning of section 2.

Theorem 2.24. *Only a finite number of fields can have the same discriminant.*

Proof : By Corollary 3 to the preceding theorem we can restrict ourselves to fields of a fixed degree, say n. We may also fix the signature $[r_1, r_2]$, and let $k = r_1 + r_2$. Let D be a fixed natural number, and let K be any field of degree n with $|d(K)| \leq D$. We shall show that $K = \mathbb{Q}(a)$, with a from a finite set depending only on D. If $r_1 \neq 0$, then define

$$X = \{[x_1, \ldots, x_{r_1}, y_{r_1+1}, z_{r_1+1}, \ldots, z_k] : |x_i| < C_i, y_j^2 + z_j^2 < 1,$$
$$i = 1, 2, \ldots, r_1; j = r_1 + 1, \ldots, k\} \subset \mathbb{R}^n$$

with $C_1 = \sqrt{D+1}$ and $C_i = 1$ for $i > 1$.

If $r_1 = 0$, then put

$$Y = \{[y_1, z_1, \ldots, y_k, z_k] : \ |y_1| < 1, |z_1| < \sqrt{D+1},$$
$$y_j^2 + z_j^2 < 1, j = 2, 3, \ldots, k\} \subset \mathbb{R}^n.$$

It is easily checked that the volumes of these sets are equal to

$$V(X) = 2^{r_1}\pi^{r_2}\sqrt{D+1}, \quad V(Y) = 4\pi^{r_2-1}\sqrt{D+1},$$

and so the quotients

$$\frac{V(X)}{2^{r_1+r_2}\sqrt{|d(K)|}} \quad \text{and} \quad \frac{V(Y)}{2^{r_2}\sqrt{|d(K)|}}$$

exceed 1. If Ψ is the map $R_K \longrightarrow \mathbb{R}^n$ defined in Lemma 2.1, then the convex body theorem implies the existence of non-zero points from $\Psi(R_K)$ in X and Y, respectively. Let a be one of them. Since the absolute values of its conjugates are bounded by a value depending only on D, the coefficients of

its minimal polynomial over $\mathbb{Q}$ are bounded, and so we get finitely many possibilities for a.

It remains to prove the equality $K = \mathbb{Q}(a)$. If $r_1 \neq 0$, then x_1 is the only conjugate of a lying outside the unit disc, since if it would lie inside or on the boundary of that disc, then we would have $|N_{K/\mathbb{Q}}(a)| < 1$. If $r_1 = 0$, then $y_1 \pm iz_1$ are the only conjugates of a having that property. Moreover $z_1 \neq 0$, since otherwise every conjugate of a would lie in the unit disc. Thus in all cases there exists a conjugate of a, distinct from all other conjugates, and so a generates K. □

2.4. Notes to Chapter 2

1. The first systematic investigation of integers lying in an algebraic number field $\neq \mathbb{Q}$ was carried out by Gauss [32], who considered integers of $\mathbb{Q}(i)$, and used them for the study of quartic reciprocity. He also suggested that numbers of the form $a + b\zeta_3$ $(a, b \in \mathbb{Z})$, i.e., integers of $\mathbb{Q}(\zeta_3)$, should be used in investigation of cubic reciprocity. He never returned to this subject himself, and the suggested study was carried out by Eisenstein [44a]. Jacobi [39] expressed the opinion that Gauss was led to complex integers through his research concerning the division of the lemniscate. In this book we shall not consider questions related to various reciprocity laws. The interested reader should turn to the book of Lemmermeyer [00], which gives a broad historical introduction into that subject.

The integers of $\mathbb{Q}(\zeta_3)$ had been earlier used by Euler [70] (see Bergmann [66a]), and integers of $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(i\sqrt{7})$ by Dirichlet ([28], [32b]) in the proof of Fermat's Last Theorem for exponents 3, 5 and 14. They did not develop the properties of the integers considered except those few which they applied directly. A study of the connection between early research concerning algebraic numbers and Fermat's Last Theorem can be found in Edwards [77].

Arbitrary quadratic fields appear first in Dirichlet [32a], who noted that expressions of the form $t + u\sqrt{a}$ with a square-free a should be subject to theorems similar to those which concern the complex integers $a + bi$. He did not suspect at that time that arithmetic in arbitrary quadratic fields may substantially differ from that in $\mathbb{Q}(i)$.

Integers of arbitrary algebraic number fields appear first in Dirichlet [46]. Dirichlet's definition of integers differs from the used today since in the field $\mathbb{Q}(a)$ he regarded as integers only elements of the ring $\mathbb{Z}[a]$, generated by a. Integers in the cyclotomic fields $\mathbb{Q}(\zeta_p)$, with prime p appear in Kummer [47a,b]. The modern definition of algebraic integers and also the definitions of the discriminant and the integral basis are due to Dedekind [71].

An early survey of the beginnings of the theory of algebraic numbers may be found in H.I.S.Smith [94]. A good insight into the early stages of this theory may be gained through Dickson *et al.* [23b]. A complete bibliography

up to 1896 is included in Hilbert's classical work (Hilbert [97]), which laid foundations for modern development.

Of the many books devoted to algebraic numbers we mention here only a selection: Artin [59], [67], Borevich, Shafarevich [64], Cassels, Fröhlich [67], H.Cohn [78], Eichler [63], Fröhlich, Taylor [93], Hasse [49], [50a], Hecke [23], Ireland, Rosen [82], Janusz [73], Koch [90], [97], Landau [18e], [27a,vol.III], Lang [64], [70], Long [77], Mann [55], Marcus [77], Mollin [99], Neukirch [92], Ribenboim [01], Samuel [67], I.Stewart, Tall [79], Swinnerton-Dyer [00], H.Weber [96b], E.Weiss [63], Weyl [40].

The modern theory of cyclotomic fields is exposed in Lang [78] and Washington [82].

Expositions of class-field theory, a subject which we shall not touch in this book, were given in Artin, Tate [68], Cassels, Fröhlich [67], Chevalley [54], H.Cohn [78], Goldstein [71c], Gras [03], Hasse [26c], [67], Iyanaga [75], Weil [67]. A new foundation of that theory, which seems to be the simplest known, was presented by Neukirch [84], [86] (cf. Neukirch [94]). For a concise survey see Narkiewicz [96].

Computational methods in algebraic number theory were treated in H.Cohen [93], [00a], Pethő, Pohst, Williams, Zimmer [91], Pohst [87], [93], Pohst, Zassenhaus [89] and Zimmer [72].

For problems and exercises see Esmonde, Murty [99].

2. The definitions of norm and trace are due to Dedekind [71]. A characterization of the norm was obtained in Artin [50b] and Flanders [53a]. The problem of finding algebraic numbers of given norm a in an algebraic number field K is easily reducible to a diophantine equation. Indeed, if $\Omega = \{\omega_1, \ldots, \omega_n\}$ is an integral basis of K, then

$$F_\Omega(X_1, \ldots, X_n) = N_{K/\mathbb{Q}}(\sum_{j=1}^{n} X_j \omega_j)$$

is an n-ary form in n variables, hence our problem consists in finding rational solutions of the equation $F(X_1, \ldots, X_n) = a$, and if one looks for integers of K with norm a, then one has to look for rational integral solution of this equation. This question has been subject to a long development and is treated e.g. in Borevich, Shafarevich [64]. See also Bartels [80], Bugeaud, Győry [96b], Garbanati [80], Győry [98a], Győry, Papp, W.M.Schmidt [72] and Siegel [73] (in case of a normal extension). Surveys were given in Evertse, Győry [88b], Győry [98b], [99].

Győry and Pethő [75], [77] considered the number $\Phi_a(t)$ of the number of solutions of $F_\Omega(X_1, \ldots, X_n) = a$, satisfying $|x_j| \leq t$, and showed that if $\Phi_a(t)$ is non-zero, then for t tending to infinity one has

$$\Phi_a(t) = c \log^r t + O(\log^{r-1} t),$$

with $c > 0$ and $r = r_1 + r_2 - 1$. Cf. Pethő [74].

Elements of an algebraic number field K which are norms in every cyclic or Abelian extension of it were studied in Ax [62]. The factor group $K^*/N_{L/K}(L^*)$, which in case of a normal extension L/K with Galois group coincides with the cohomology group $H^0(G, K^*)$, was considered in Hürlimann, Saltman [85], Opolka [87], [91]. This factor group is infinite, as shown in Stern [90] (cf. Hutchinson [95a]).

An extension L/K is called *solitary* if for any finite extension M/K satisfying $N_{L/K}(L^*) = N_{M/K}(M^*)$ follows that the extensions L/K and M/K are isomorphic. For Galois extensions this was considered in Guralnick, Stern [95] and Stern [89], and the non-Galois case was treated in Stern [99]. See also Coykendall [96], [00].

A formula for the index of $T_{L/K}(R_L)$ in R_K in the case when $L/\mathbb{Q}$ is Abelian and $K \subset L$, was proved in Girstmair [92b].

There are only finitely many algebraic integers of given degree, discriminant and norm (Győry [73], see also Győry [81a], [81b], [83], [84], Győry, Papp [77], [83], where also certain generalizations have been considered). For the cubic case see Delaunay Faddeev [40], Nagell [30].

Schur [18a] proved that if $c < \sqrt{e} = 1.6847\ldots$, then only finitely many totally real and totally positive integers of degree n can have their trace smaller than cn. Siegel [45a] proved that for $c = 3/2$ the only such integers are 1 and $(3 \pm \sqrt{5})/2$, and conjectured that for any $c < 2$ there are only finitely many such numbers. See Dinghas [52], Hunter [56], Smyth [84a].

Totally positive integers with a given trace in a totally real field were studied in Behnke [23]. It has been shown in de Smit [93] that if α is an algebraic number of degree n such that the powers α^i have integral traces for $i = 1, 2, \ldots, n + \log_2 n$, then α is an algebraic integer.

The book of Conner and Perlis [84] is devoted to the study of the quadratic form $T_{K/\mathbb{Q}}(x^2)$, which arises when $x \in R_K$ is written in the form $x = \sum_{j=1}^{n} x_j \omega_j$, where $\{\omega_j\}$ is an integral basis of K. Schinzel [75a] considered the function $T_{K/\mathbb{Q}}(f(X))$ for a polynomial $f \in K[X]$, and showed that in case of a real field K it cannot be negative for all values of $x \in K$. Cf. Bazylewicz [82].

Lemma 2.3 is very old (cf. Coolidge [08], Cucker, Corbalan [89], Kneser [42]).

3. Theorem 2.5 was proved by Kronecker [57a]. Other proofs of part (i) were given in Greiter [78] and Spencer [77], and of part (ii) in Lehmer [32]. Schur [18a] generalized part (ii) by showing that an interval on the real axis of length smaller than 4 can contain only a finite number of full sets of conjugates (FCS) of an irrational algebraic integer, and this was put in a broader context by Fekete [23]. He proved that every compact subset of the complex plane with transfinite diameter less than 1 can contain at most finitely many FCS. Since the transfinite diameter of a real interval of length a equals $4a$, this generalizes Schur's result. A further generalization, relating the problem to

Julia sets, arising in the study of polynomial dynamics, appears in Moussa, Geronimo, Bessis [84]. See also Flammang, Rhin, Smyth [97].

A plane analogue of Theorem 2.5 is due to Fekete and Szegö [55]: if E is a set on the complex plane, closed under conjugation. whose interior contains a subset with transfinite diameter equal 1, then E contains infinitely many FCS. (For far reaching generalizations see Cantor [80], Chinburg [91], Rumely [89], [00], Rumely, Lau, Varley [00]). Another proof of Theorem 2.5 appears in Cantor [80]. There is no analogue of the Fekete-Szegö theorem for real sets, since there are such sets with arbitrary large transfinite diameter, not containing any algebraic numbers (Robinson [64a]; cf. Robinson [64b,c]).

Ennola [75a] showed, confirming a conjecture of Robinson [62], that in Theorem 2.5 the resulting FCS may consist of numbers having an arbitrary sufficiently large degree. Therefore, if $I(n)$ denotes the smallest positive number such that every closed interval of length $\geq I(n)$ contains FCS of an integer of degree n, then $\lim_{n\to\infty} I(n) = 4$. For infinitely many n one has

$$I(n) \leq 4 + 4\frac{(\log\log n)^2}{\log n}$$

(Dubickas [00a]), and $I(2) = \sqrt{2} + (1+\sqrt{5})/2$ (Dubickas [99]).

Straight lines containing infinitely many FCS were described in Motzkin [45], and circles with that property were dealt with in Robinson [69], Ennola [73a], Ennola, Smyth [74], [76]. The same problem for arbitrary conics was studied in Smyth [82]. For similar questions see Cantor [76], Ferguson [70], Greaves, Odoni [88], Nishizawa, Sekiguchi, Yoshino [91], Odoni [91a], Robinson [67], J.G.Thompson [93].

Theorem 2.3. obviously fails for non-integers. Indeed, there are plenty of algebraic numbers a with $\overline{|a|} = 1$ which are not roots of unity, and it was shown in Blanksby, Loxton [78] that a totally complex field K is a quadratic extension of a totally real field (such fields are called CM-fields) if and only if $K = \mathbb{Q}(a)$ with $\overline{|a|} = 1$ and $a \neq \pm 1$. Numbers having some conjugates on the unit circle were considered in Halter-Koch [71a]).

It has been proved in Motzkin [47] that if $z_1, z_2, \ldots, z_{n-1}$ is a given set of complex numbers, closed upon conjugation, then for every $\epsilon > 0$ one can find an algebraic integer a of degree n, whose conjugates $a_1 = a$, $a_2, \ldots, a_n$ satisfy $|a_i - z_i| < \epsilon$ for $i = 1, 2, \ldots, n-1$.

4. In this subsection we shall assume that a is a non-zero algebraic integer of degree n, which is not a root of unity. For such numbers one defines its *Mahler's measure* $M(a)$ by the formula

$$M(a) = \prod_{i=1}^{n} \max(1, |a_i|),$$

where $a = a_1, a_2, \ldots, a_n$ are all conjugates of a over $\mathbb{Q}$. Lehmer [33a] asked, whether for every $\epsilon > 0$ there exists a with $1 < M(a) < 1 + \epsilon$, but nowadays

one believes generally that the converse is true, and therefore the following assertion is known as *Lehmer's Conjecture*:

There exists a constant $C > 0$ such that one has

$$M(a) \geq 1 + C. \tag{2.9}$$

The smallest known value of $M(a)$ is $1.176\ldots$, realized by a root of the polynomial $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$ (Lehmer [33a]).

Lehmer's conjecture is related to a question posed by Schinzel and Zassenhaus [65], who proved that if a has $2s$ non-real conjugates, then

$$\overline{|a|} \geq 1 + 4^{-s-2}$$

holds. They asked whether there exists a positive constant c such that for every non-zero integer a of degree n, which is not a root of unity, one has

$$\overline{|a|} \geq 1 + \frac{c}{n}. \tag{2.10}$$

It has been shown in Pinner, Vaaler [99] that this problem is equivalent to a question about the number of irreducible factors of a polynomial with coefficients in an algebraic number field. If Lehmer's conjecture turns out to be correct, then we would have also a positive answer to the question of Schinzel and Zassenhaus with $c = \log(1 + C)$, due to the obvious inequality

$$M(a) \leq \overline{|a|}^n.$$

A polynomial P of degree N is said to be *reciprocal*, if $P(X) = X^N P(1/X)$. Breusch [51] and Smyth [71] showed that Lehmer's conjecture holds for those a's, whose minimal polynomials are non-reciprocal, and in Blanksby [69] it was shown that the same holds in the case when a has many real conjugates. Smyth proved also that the minimal value of $M(a)$ for these a's equals $\theta = 1.3247\ldots$, realized by a root of $X^3 - X - 1$. and this implies

$$\overline{|a|} \geq 1 + \frac{\log \theta}{n} = 1 + \frac{.281\ldots}{n}.$$

For large n the constant .281 has been improved in Dubickas [97c] to .3096. Cassels [66] proved that in this case (2.10) holds with $c = 1/10$, and in Schinzel [69] this constant was doubled.

For an analogue in the case of roots of non-reciprocal polynomials with coefficients in a totally real field see Schinzel [73], Bazylewicz [76].

In Blanksby, Montgomery [71] the inequality

$$M(a) \geq 1 + \frac{1}{52} \frac{1}{n \log(6n)}$$

was obtained, and this has been improved by E.Dobrowolski, who first established Theorem 2.4 (Dobrowolski [78]), and then showed (Dobrowolski [79]) that for $n \to \infty$ one has

$$M(a) \geq 1 + c_1 \left(\frac{\log\log n}{\log n} \right)^3 \tag{2.11}$$

with $c_1 = 1 + o(1)$ (he pointed out that for all n one can take $c_1 = 1/1200$), and

$$\overline{|a|} \geq 1 + \frac{c_2}{n} \left(\frac{\log\log n}{\log n} \right)^3 \tag{2.12}$$

with $c_2 = 2 + o(1)$. Up to the value of the constants c_1, c_2 this remains still the best step towards Lehmer's conjecture. The largest known value of c_1 is $2.45 + o(1)$ (Louboutin [83]), and that of c_2 is $64/\pi^2 + o(1)$ (Dubickas [93]). Previous results gave $c_1 = 2 + o(1)$ (Cantor, Straus [88], Rausch [85]). See C.L.Stewart [78] for a proof of $M(a) \geq 1 + \frac{C}{n \log n}$ with $C = 10^{-4}$ and Matveev [91] for an improvement of the constant in Theorem 2.4 for $n \leq 2300$. Explicit bounds gave Voutier [96], who obtained a.o. $\log M(a) \geq 0.25(\log\log n/\log n)^3$ for $n \geq 2$.

Amoroso [98] gave an upper bound for the resultant of two polynomials, and this led to a new proof of the theorem of Dobrowolski.

There are also analogues of the above results in the case of totally real integers a of degree n, which are not of the form $a = \cos(2\pi r)$ with rational r. Already in Schinzel, Zassenhaus [65] it has been established that in that case

$$\overline{|a|} > 2 + \frac{1}{4^{2n+3}}.$$

Later

$$\overline{|a|} \geq 2 + \frac{1}{300 n^2 \log^2 n}$$

was proved (Blanksby, Montgomery [71]), and the strongest known result is due to Dubickas [95b], who proved

$$\overline{|a|} \geq 2 + \frac{3.8}{n} \frac{(\log\log n)^3}{\log^4 n},$$

and in [97b] showed that for large n the constant 3.8 can be replaced by 4.6. Cf. Smyth [80], Flammang [96] for a search of totally real and totally positive integers of small Mahler's measure. For numerical results see Boyd [80], [85].

It is clear that Mahler's measure of an algebraic integer a depends only on the minimal polynomial of a, and therefore one can extend its definition to all polynomials $P(X) = a_n X^n + \cdots + a_0$ with rational integral coefficients by putting

$$M(P) = |a_n| \prod_{j=1}^{n} \max\{1, \alpha_j\},$$

where $\alpha_1, \ldots, \alpha_n$ are roots of P, taken with appropriate multiplicities. It is not difficult to see that Mahler's measure can be also defined analytically by the formula

$$M(P) = \exp\left(\int_0^1 \log(|P(e^{2\pi it})|)dt\right),$$

and it has been established by Szegö [15] that if for a polynomial P we put

$$\| P \|_2 = \left(\int_0^1 |P(e^{2\pi it})|^2 dt\right)^{1/2},$$

then one has

$$M(P) = \inf\{\| PQ \|_2\},$$

where Q runs over all complex polynomials. with $Q(0) = 1$. For an extension to several variables see Ruzsa [99].

Limit points of the set $\{M(P) : P \in \mathbb{Z}[X]\}$ were studied in Boyd [81a]. Lower bounds for $M(P)$ depending on the number of non-zero coefficients were established in Dobrowolski, Lawton, Schinzel [83] and Dobrowolski [91].

For other results concerning $M(a)$ and $\overline{|a|}$ see Amara [79], Amoroso [95], [96], Boyd [86a,b], Boyd, Villegas [02], Brunotte [80], [82], Bugeaud [98], Bugeaud, Mignotte, Normandin [95], Dubickas [97a], [98], [00b], [01], [02a,b], Dubickas, Konyagin [98], Dubickas, Smyth [01c], Flammang [97], Glesser [89], Langevin [86], Lloyd-Smith [85a], Matveev [99], Notari [78], Panaitopol [00], Pathiaux [75], Rhin, Smyth [95], [97], Schinzel [73,addendum], Silverman [95], [96], Zheludevich [91].

In the case of polynomials in several variables one defines Mahler's measure in the following way: if $P(z_1, \ldots, z_n)$ is a non-zero polynomial with complex coefficients, then

$$M(P) = \exp\left(\int_0^1 \cdots \int_0^1 \log(|P(e^{2\pi it_1}, \ldots, e^{2\pi it_n})|)dt_1 \cdots dt_n\right).$$

Actually, this is the original definition, given by Mahler [62] for his measure. An analogue of Kronecker's theorem in this case were obtained in Boyd [81b] and Smyth [81a]. Boyd's paper contains also lower bounds for $M(P)$. There are unexpected relations between values of $M(P)$ for polynomials in two variables and special values of holomorphic functions, occurring in number theory. E.g., one has

$$\log M(1 + X + Y) = \frac{3\sqrt{3}}{4\pi} \sum_{m=1}^{\infty} \frac{\chi(m)}{m^2},$$

where $\chi(m)$ is the non-principal Dirichlet character mod 3, and

$$\log M(1 + X + Y + Z) = \frac{7\zeta(3)}{2\pi^2}.$$

(Smyth [81b]).

For other examples, generalizations, numerical experiments, results and conjectures see Amoroso, David [99], Amoroso, Dvornicich [00], Amoroso,

Zannier [98], [00], Bertin [01], Boyd [98a,b], [99], [02], Deninger [97], Dubickas, Smyth [01a,b], Mossinghoff [98], Ray [87], Villegas [99].

Mahler's measure turned out to be of importance also in other parts of mathematics (see Einsiedler [99], Everest [98], Everest, Ward [99], Lind [74], Lind, K.Schmidt, Ward [90], Maillot [00]).

For various mean values of the conjugates of algebraic integers see Flammang [95], Smyth [84b].

Kronecker constant $\epsilon(K)$ is defined as the largest lower bound for $\overline{|a|}-1$, where a ranges over all non-zero integers $a \in K$, which are not roots of unity. Callahan, Newman, Sheingorn [77] proved that every field can be embedded in a field K with $\epsilon(K) \geq 2^{1/n}-1$, where $n = [K : \mathbb{Q}]$. They quote the following question of Bateman: does $\epsilon(K) = 1$ hold for most fields K? It holds for all fields of prime degree and sufficiently large discriminant. Cf. Robinson [65].

5. If $\alpha_1 = \alpha, \ldots, \alpha_n$ is a complete set of conjugates of a non-zero non-rational algebraic integer of degree n, then write $d(\alpha) = \max_{i,j} |\alpha_i - \alpha_j|$, and put $D(n) = \inf_{\deg a = n} d(\alpha)$. Favard [29], [30] noted that $d(\alpha) > \sqrt{1.5}$. This was improved in Lloyd-Smith [84] to $d(\alpha) > 1.5$, in McAuley [81] to $d(\alpha) > 1.659$ (cf. Blanksby, Lloyd-Smith, McAuley [89]), and the final step was done by Langevin, Reyssat and Rhin [88], who proved the inequality $d(\alpha) \geq \sqrt{3}$, which is best possible, the equality being realized by the third root of unity. Moreover one has $\lim_{n\to\infty} D(n) = 2$ (Langevin [88a]), and the same is true if one considers conjugates over an imaginary quadratic field (Langevin [88c]; see also Langevin [88b]). If α lies in a CM-field, then one has, except for certain exceptional α's, $d(\alpha) \geq 2.7587\ldots$ (Lloyd-Smith [85b]). If we put $D^+(n) = \inf_{\substack{\deg \alpha = n \\ \alpha \text{ tot.real}}} d(\alpha)$, then $\lim_{n\to\infty} D^+(n) = 4$ and $D^+(5) \geq 3.18$ (Zaïmi [94]). The minimal value of $|\alpha_i - \alpha_j|$ was considered by Rump [79]. For similar questions see Blanksby [70], Dubickas [95a], Grandcolas [98a,b], Hunter [56].

6. A real algebraic integer is called a *Pisot number* or a *PV-number* if it exceeds 1 and its remaining conjugates lie inside the unit disc. They were studied by Pisot [36] and Vijayaragavan [40], but for the first time they occurred in Thue [12] and Hardy [19]. These numbers have remarkable properties, e.g. they form a closed set (Salem [44]). An integer > 1 is called a *Salem number* if it is not a Pisot number, and its remaining conjugates lie in the closed unit disc (Salem [45]). Interesting relations occur between these classes of numbers and harmonic analysis. There is a large literature on this topic and the interested reader should consult the books of Bertin, Decomps-Guilloux, Grandet-Hugot, Pathiaux-Delefosse, Schreiber [92], Bertin, Pathiaux-Delefosse [89], Meyer [70], Pisot [63], Salem [63].

7. The main notions and results of Sect.2, in particular the fundamental Theorem 2.10, are due to Dedekind [71]. This theorem was generalized in Stiemke [26], who proved that every additive group consisting of algebraic integers is free. Moreover (C.U.Jensen [64]), if L/K is an infinite algebraic

extension of an algebraic number field, then algebraic integers contained in L form a free R_K-module. For a simple proof see Kulkarni [67]. Various methods of finding integral bases were proposed in Albert [37], Berwick [27], Canals, Ortiz [70], Ore [25b], Petr [35], N.R.Wilson [27], [31], Zassenhaus [65]. Some of these methods could be used for finding $\mathbb{Z}$-bases of ideals (see Eda [53], Mann, Yamamoto [67], McDuffee [31], Nagell [65], N.R.Wilson [29]). Bases of ideals satisfying certain inequalities were constructed by Mahler [64], who used them to deduce anew various fundamental results of the theory of algebraic numbers. Cf. Luthar [66].

For a generalization of Proposition 2.13 to arbitrary extensions see Fuchs [48].

If $K/\mathbb{Q}$ is a normal extension of prime power degree, then, as shown in de Smit [95], every integral basis of K contains a generator of K. This holds also for certain other classes of fields, but fails for dihedral fields of degree 12.

8. Several papers were concerned with discriminants and integral bases of particular classes of fields.

(a) *Cubic fields.* Elementary treatments of arithmetics in cubic fields were given in Châtelet [46] for normal fields, and in Reichardt [33] in the general case (see also Nagell [30]). The non-normal case was treated from the point of view of class-field theory in Hasse [30b].

Algorithms and even explicit formulas for integral bases were given already by Voronoi [96] (see Sommer [07], Delaunay, Faddeev [40]). Cf. also Albert [30b], Arai [81], Bergström [37], Mathews [93], Shapiro, Sparer [91], Spearman, Williams [98], Tornheim [55].

A list of cubic fields with small discriminants is given in H.Cohen [93]. Real cubic fields with $d(K) < 500\,000$ are listed in Ennola, Turunen [85].

Normal cubic fields are characterized by the fact that their discriminants are squares (see Corollary 2 to Proposition 6.9). Squares which are such discriminants were described in Hasse [48a] (see Girstmair [79] for a simple proof). Discriminants of non-normal cubic fields were described in Martinet, Payan [67] and Satgé [81] (cf. also Llorente, Nart [83]).

Let $A(d)$ be the number of non-isomorphic cubic fields with discriminant d. This function, which, contrary to the quadratic case, is unbounded, was studied in Berwick [24], Hasse [30b], Martinet, Payan [67]. Asymptotics for the sum $\sum_{|d|\leq x} A(d)$ was found in Davenport, Heilbronn [69]. For a numerical test of a more precise conjectural formula see Roberts [01]. Earlier H.Cohn [54] proved a similar result for cyclic cubic fields. Computations of cubic fields were done in Angell [76], Belabas [97], Fung, Williams [90]. For a generalization of the Davenport-Heilbronn result to arbitrary base fields see Datskovsky, Wright [88].

(b) *Quartic fields.* It is a simple exercise to show that a quartic normal field with Galois group isomorphic to $C_2 \oplus C_2$ has the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, where

a, b are rational integers whose product is not a square. Such fields are called *biquadratic*. The general form of a quartic cyclic field is $\mathbb{Q}\left(\sqrt{a(d+b\sqrt{d})}\right)$, with $a, b, d \in \mathbb{Z}$, with a odd and square-free, $(a, d) = 1$, $b \neq 0$, d square-free and such that $d - b^2$ is a non-zero square (see Hardy, Hudson, Richman, Williams, Holtz [86]; for other forms cf. Edgar, Peterson [80], Nagell [62], Tang [91], Zhang X. [84d]).

Tables of quartic fields with small discriminants were given in Godwin [56], [57a,b], Kwon [84] and Pohst [75a]. In Buchmann, Ford [89], Ford [89] and Buchmann, Ford, Pohst [93] all quartic fields K with $|d(K)| < 10^6$ were enumerated.

Discriminants and integral bases of quartic fields were given in Grebenyuk [58], Albert [30a] in case of normal extensions (note, however, that some of his results are incorrect, as pointed out by Zhang X. [84a]), Hudson, Williams [90] for cyclic fields, Amberg [97], Litver [55] and K.S.Williams [70] for biquadratic fields, Huard, Spearman, Williams [95] for fields containing a quadratic subfield (for an earlier partial result see Ledermann, van der Ploeg [85]), Funakura [84] for pure quartics.

Asymptotics for the number of integers which are discriminants of normal quartic fields was found in Spearman, Williams [01a], and asymptotics for the number $M(x)$ of quartic fields K with $|d(K)| \leq x$, whose Galois closure has a given Galois group was considered by Baily [80], who proved

$$x \ll M(x) \ll x^{3/2} \log^4 x.$$

(c) *Quintic fields.* Tables of cyclic quintic fields with small discriminant were given in A.Schwarz, Pohst, Diaz y Diaz [94].

Cyclic quintic fields were studied in Payan [62a,b]. A formula for the discriminant of a quintic field defined by a trinomial $X^5 + aX + b$ whose Galois group is dihedral was given in Spearman, Williams [02a].

(d) *Sextic fields.* Integral bases for sextic fields with Galois group C_3^2 were given in Parry [90]. Sextic fields of small discriminant were tabulated in a series of papers of Olivier [89], [91a,b]. For fields with a quadratic subfield this was made in Bergé, Martinet, Olivier [90]. A theory of normal nonabelian sextic fields was developed in Martinet, Payan [67], [68].

(e) *Other classes of fields.* Arithmetic in arbitrary abelian extensions $K/\mathbb{Q}$ was described by Leopoldt [59], [62], who gave, in particular, explicit integral bases in terms of Gaussian sums. For the case of cyclic extensions of odd prime degree see Payan [65], and of prime power degree see Oriat [72].

Discriminants and integral bases for pure fields $\mathbb{Q}(\sqrt[m]{a})$ $(a \in \mathbb{Z})$ were for square-free m found in Berwick [27], and in the case $(a, m) = 1$ in Okutsu [82]. The case of prime m was settled earlier by Landsberg [97]. Composites of quadratic fields were treated in Schmal [89]. Discriminants of solvable fields

of prime degree were found in F.K.Schmidt [29], Wegner [32a] and Hasse [37], and integral bases for them gave Komatsu [76b].

All sextic and septic fields with discriminants of the form $\pm 2^a 3^b$ were found in Jones, Roberts [99], [03]. Septic fields with discriminant $\pm 7^a$ were determined in Bruegeman [01], who also proved that there are no such fields with discriminant $\pm p^a$ with $p = 2, 3, 5$.

For various special types of fields see Foster [70], Komatsu [75], [76a], Llorente, Nart, Vila [84], Watanabe [92].

Tables for fields of degree 10 having a quintic subfield with either $r_1 = 1$ or $r_1 = 5$ were computed in Selmane [01a,b].

Tables of totally complex fields of degree ≤ 80 having small discriminants were prepared by H.Cohen, Diaz y Diaz, Olivier [98b].

If $N(n, x)$ denotes the number of non-isomorphic fields of degree n with $|d(K)| \leq x$, then one has $N(n, x) \ll x^{(n+2)/4}$ (W.M.Schmidt [95]).

9. Theorem 2.14 is due to L.Stickelberger [97], and the presented proof was found by Schur [29b].

Using the theory of the different (see Chap. 4) one can obtain more information about discriminants. On this topic see Bauer [19a], Hensel [97a], Ore [25b], [26c,d], Schur [32]. We quote one of results of Ore [26c]: if $n = \sum_{j=0}^{N} b_j p^j$ with $0 \leq b_j < p$, and A denotes the number of non-zero b_j's, then the maximal power of p dividing the discriminant of a field of degree n cannot exceed $N(n, p) = \sum_{j=0}^{N} (j+1) b_j p^j - A$, and this bound is attained. Integers $k \in [0, N(n, p)]$ for which there exists a field K of degree n with $p^k \parallel d(K)$ were determined in W.R.Thompson [31].

10. *Power bases.* Proposition 2.21 is due to Hensel [94b]. Győry [73,III] proved that if F is an index form, then the equation $F = a$ has for non-zero $a \in \mathbb{Z}$ only finitely many solutions, and gave a bound for them. This bound was later improved in Bérczes [00]. For surveys of results concerning index form equations see Evertse, Győry [88b], Győry [00]. For certain classes of fields relevant algorithms were given in Gaál [95], Gaál, Győry [99], Gaál, Pohst [96], Járási [02].

Primes dividing values of the index form were studied in Győry, Papp [77] and Trelina [77b].

It follows from a theorem of Uchida [77b] that $R_K = Z[a]$ holds if and only if a generates K, and its minimal polynomial over $\mathbb{Z}$ is not contained in the square of a maximal ideal of $\mathbb{Z}[X]$ (cf. Albu [79]).

It is clear that a field K has a power basis if and only if there exists a monic irreducible polynomial over $\mathbb{Z}$, whose discriminant equals $d(K)$, and which has a root θ with $\mathbb{Q}(\theta) = K$. The question of the existence of a non-monic polynomial with there properties was considered in Simon [01].

Algorithms for determining all power bases in fields of degree ≤ 6, and in some classes of octic and nonic fields (in the case when they exist) were

given in the book of Gaál [02], where also references to previous research can be found.

Cyclic cubic monogenic fields were described in Archinard [74], M.N.Gras [74] and Payan [73]. There are only two complex cyclic monogenic quartic fields (M.N.Gras [81]), but there are infinitely many such biquadratic fields (Nakahara [83]) (a criterion in this case was given in M.N.Gras, Tanoé [95]; cf. Nyul [01]), as well as pure quartic fields (Funakura [84]). For cyclic quartic fields see also Nakahara [93]. A criterion in case of quartic fields whose Galois closure is dihedral appeared in Kable [99], and was applied in Gaál, Nyul [01]. A method for finding all power integral bases in a quartic field gave Koppenhöfer [95]. For cyclic sextics see Shah [00]. Necessary conditions for monogenity for certain classes of sextic fields were given in Chang [02] and Thérond [95], [99]. For sufficient conditions in the case of sextic fields with a cubic subfield see Járási [03]. A necessary and sufficient condition for monogenity of a cyclic field of prime degree appears in Payan [73], where also cyclic extensions of imaginary quadratic fields were considered (cf. Cougnard [88]).

There are only finitely many monogenic Abelian fields of a fixed degree prime to 6 (M.N.Gras [84]), and they can be determined. It has been shown in Liang [76] that maximal real subfields of cyclotomic fields are monogenic. The only monogenic cyclic fields of a prime degree $p \geq 5$ are the maximal real subfields of $Q(\zeta_q)$, where $q = 2p+1$ is a prime (M.N.Gras [86a]), and a similar result holds for cyclic p-extensions of $\mathbb{Q}$ (M.N.Gras [86b]). For dihedral and imaginary cyclic extensions of degree $2p$ see Cougnard [87a,b]

If K is monogenic and $R_K = \mathbb{Z}[a]$, then for $m \in \mathbb{Z}$ one has also $R_K = \mathbb{Z}[a+m]$. The resulting power bases are called *equivalent*. Nagell [68b] asked, whether integers of a given degree with a given discriminant form a finite number of classes, two integers lying in the same class if and only if they differ by a rational integer (a similar idea appears already in a letter of Hermite [57] to Borchardt). He confirmed it for degrees ≤ 4, and the general case was settled by Győry [73] in an effective way. This follows also from a result of Birch, Merriman [72], which, however, was not effective. This implies that in a given field there can be only finitely many pairwise inequivalent power bases. Cf. Győry [79a], [80a,b], [81a,b], [83], [84], Győry, Papp [77], Trelina [77a,b].

It has been conjectured by Bremner [88] that in the p-th cyclotomic field there are only two inequivalent power bases. This holds for all $p \leq 23$ (Bremner [88], Robertson [98], Wildanger [00]). All power bases in $\mathbb{Q}(\zeta_{2^m})$ were described in Robertson [01].

For certain other classes of fields see Dummit, Kisilevsky [77], Gaál, Olajos, Pohst [01], Ichimura [00a,b], [01a], Ichimura, Sumida [00], Motoda, Nakahara, Shah [02], Nyul [02], Shah, Nakahara [02], Spearman, Williams [01b].

Power bases in composita of fields were considered in Gaál [98].

For power bases in ray class-fields of imaginary quadratic fields see Sect. 4.4.

Monogenity of a field is closely connected with the notion of canonical number systems. If R is a domain, $c \in R$, and $A \subset \mathbb{Z}$ is finite, then the pair (c, A) is called a *canonical number system*, if every element a of R can be written in the form $a = \sum a_j c^j$ $(a_j \in A)$ in a unique way. It has been shown in Kovács, Pethő [91] that the only domains which can have canonical systems are $\mathbb{Z}[a]$ (with algebraic a) and $\mathbf{F}_p[X]$, This paper contains also a method of finding all such systems. Cf. Indlekofer, Kátai, Racskó [92], Kátai [94], Kátai,, Kőrnyei [92], Kovács [81], Kovács, Pethő [92], Scheicher [97]. It follows that K is monogenic if and only if R_K has a canonical number system.

The minimal number of generators of R_K (as a ring) was determined by Pleasants [74].

11. It follows from a result of Lewin [67] that R_K can have only finitely many subrings of a given index (cf. Nagell [32], [65]). Such subrings containing 1 are called *orders* of K, and R_K is called sometimes the *maximal order* of K. For their theory see e.g. Dedekind [78], Grell [27], [36b], Krull [28c], Nagell [32]. A classification of subrings of R_K spanning K as a vector space was given in Beaumont, Pierce [61] (cf. Krull [28a], Skolem [23]).

12. *Discriminant evaluations.* Theorem 2.22 was proved by Minkowski [91b]. Its Corollary 2 was stated without proof by Kronecker [82], and proved in Minkowski [91a]. Other proofs of that corollary can be found in Calloway [55], Landau [22], Mordell [22b], [31], Müntz [23], Odlyzko [76], Schur [18a], Weber, Wellstein [13]. For special cases see Lubelski [39a], Siegel [22a]. Theorem 2.24 is due to Hermite [57].

One sees easily that $M(2,0) = 5$ and $M(0,1) = 3$. For cubic fields we have $M(1,1) = 23$ and $M(3,0) = 49$, realized by $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = 1 + \alpha$ and $\alpha^3 = -\alpha^2 + 2\alpha + 1$, respectively (see e.g. Cassels [59b]).

Moreover $M(0,2) = 117$, $M(2,1) = 275$, $M(4,0) = 725$ (Mayer [29]), $M(1,2) = 1609$, $M(3,1) = 4511$, $M(5,0) = 14641$ (Hunter [57]), $M(0,3) = 9747$ (Liang, Zassenhaus [77]), $M(2,2) = 28037$, $M(4,1) = 92\,779$ (Pohst [82]), $M(6,0) = 300\,125$ (Pohst [75b]), $M(7,0) = 20\,134\,393$ (Pohst [76]), $M(5,1) = 2\,306\,559$ (Diaz y Diaz [88]), $M(3,2) = 612\,233$ (Diaz y Diaz [84]), $M(1,3) = 184\,607$ (Diaz y Diaz [83]), $M(8,0) = 282\,300\,416$ (Pohst, Martinet, Diaz y Diaz [90]), $M(0,4) = 1\,257\,728$ (Diaz y Diaz [87]), $M(9,0) = 9\,685\,993\,193$ (K.Takeuchi [99]; earlier Letard [95] obtained this assuming *GRH*).

Minimal discriminants of various classes of sextic fields were given in Ford [96], Ford, Pohst [92], [93], Ford, Pohst, Daberkow, Haddad [98]. Minimal discriminants of octic fields containing a quartic subfield (for all signatures and Galois groups) were found in H.Cohen, Diaz y Diaz, Olivier [99]. For some other classes of octic fields this was done in Selmane [99]. The minimum of $|d(K)|$ for cyclic K of prime degree p equals q^{p-1}, with q being the smallest

prime $\equiv 1 \bmod p$ if $q < p^2$, and equals $p^{2(p-1)}$ otherwise (Kostra [89]). Minimal discriminants for normal fields with quaternion groups of order 8, 12 and 20 were found by Kwon [96]. The first five minimal discriminants of nonic fields having a cubic subfield were found in Fujita [93] (cf. Diaz y Diaz, Olivier [95]).

If $n = 2r_1 + r_2$, then for large n one has

$$M(r_1, r_2) \geq c(60.1)^{r_1}(22.2)^{r_2}$$

(with $c = \exp(-254)$), as shown by Odlyzko [75], [76], [77], and under *GRH* one can even have

$$M(r_1, r_2) \geq c_1(188.3)^{r_1}(41.6)^{r_2}$$

with $c_1 = \exp(-3.7 \cdot 10^8)$ (Odlyzko [76], [77]). Later Poitou [76] got

$$D = \liminf_{n\to\infty} M(r_1, r_2)^{1/n} \geq 22.3,$$

and $D \geq 44.7$ under *GRH* (cf. Martinet [82].) For early surveys of this topic see Martinet [85], Odlyzko [90], Poitou [77].

It has been conjectured for a long time that $D = \infty$, however already Siegel [45a] mentioned that this may be false, and later Golod and Shafarevich [64] proved $D \leq 4404.5$. This was later improved to $D \leq 347$ (Brumer [65]), $D \leq 92.369$ (Martinet [78]), and $D < 82,2$ (Hajir, Maire [01,II]). See also Martinet [79b], [82].

Lower bounds for discriminants of metabelian fields obtained Ankeny [51].

EXERCISES

1. Prove that if an algebraic integer a is totally real and totally positive, and $f(X) = X^n + \sum_{j=0}^{n-1} a_j X^j$ is its minimal polynomial over $\mathbb{Z}$, then one has $(-1)^k a_k > 0$ for $k = 0, 1, \ldots, n-1$.

2. Put $\epsilon(K) = \inf\{|\overline{a}| - 1 : a \in R_K, a \neq 0, a \text{ not a root of unity}\}$.

(i) Determine $\epsilon(K)$ for quadratic fields.

(ii) (Callahan, Newman, Sheingorn [77]) Prove that if $K/\mathbb{Q}$ is normal and the complex conjugation lies in the centre of $Gal(K/\mathbb{Q})$, then $\epsilon(K) \geq \sqrt{2} - 1$.

3. (Blanksby, Loxton [78]) Prove that a non-real field K is closed under complex conjugation if and only if K is generated by an element of absolute value 1. (Hint: look at elements of the form $(a + r)(\bar{a} + r)$, where a generates K and $r \in \mathbb{Q}$).

4. (Smyth [73]) Prove that if a is a Pisot number, and two of its distinct conjugates, say a_i and a_j have the same absolute value, then $a_j = \bar{a}_i$.

5. Prove that every real field can be generated by a Pisot number, and show that this does not hold for Salem numbers.

6. (i) Prove that a ring $R \subset R_K$ is an order of K if and only if it contains $[K : Q]$ elements linearly independent over $\mathbb{Q}$ and $1 \in R$.

(ii) Let d be a square-free rational integer. Prove that every order in the field $\mathbb{Q}(\sqrt{d})$ has the form $O_N = \{a + bN\omega : a, b \in \mathbb{Z}\}$ for some $N \geq 1$, with $\omega = (1 + \sqrt{d})/2$ in the case $d \equiv 1 \pmod 4$ and $\omega = \sqrt{d}$ otherwise.

7. (i) Prove that if $K = \mathbb{Q}(a)$ is normal of degree n, then $d(K)$ is a square if and only if the Galois group of $K/\mathbb{Q}$, treated as a permutation group of conjugates of a, is contained in the alternating group A_n.

(ii) Prove that if $K/\mathbb{Q}$ is normal of odd degree, then $d(K)$ is a square, and for cubic extensions the converse holds.

7. Determine the discriminant and find an integral basis for the field $\mathbb{Q}(i, \sqrt{m})$, where $m \neq \pm 1$ is a square-free rational integer.

8. Find the discriminant and an integral basis for the maximal real subfield of $\mathbb{Q}(\zeta_p)$, where $p \neq 2$ is a prime.

9. Let L/K be of degree n.

(i) Show that R_L can be generated, as an R_K-module by at most $1+n$ elements.

(ii) Prove that R_L has a set of n generators as a R_K-module if and only if it is a free R_K-module.

3. Units and Ideal Classes

3.1. Valuations of Algebraic Number Fields

1. Consider an algebraic number field K. We know already from Corollary to Theorem 1.20 that its ring of integers is a Dedekind domain with the finite norm property. This allows us to construct discrete valuations of K using the exponents associated to prime ideals of R_K. In this section we shall examine all valuations of K, including the Archimedean, and we shall establish that every Archimedean valuation of K is generated by an embedding of K in $\mathbb{C}$, whereas every other non-trivial valuation is discrete and induced by a prime ideal of R_K.

The reader should be warned that a similar result is not necessarily true for other fields. Indeed, consider the field $\mathbb{C}(X)$ of rational functions in one complex variable. We shall show that it contains no Dedekind domain, whose prime ideals induce all discrete valuations, The formula $\nu(P/Q) = \deg Q - \deg P$, where P, Q are relatively prime polynomials, defines an exponent in $\mathbb{C}(X)$. Moreover for any $z \in \mathbb{C}$ we have an exponent n_z defined by

$$n_z(P/Q) = \begin{cases} r & \text{if } P(X) = (X-z)^r P_1(X), P_1(z) \neq 0, \\ -r & \text{if } Q(X) = (X-z)^r Q_1(X), Q_1(z) \neq 0, \\ 0 & \text{if } P(z)Q(z) \neq 0. \end{cases}$$

Assume now that R is a Dedekind domain, having $\mathbb{C}(X)$ for its quotient field, and whose prime ideals induce ν and n_z for all $z \in \mathbb{C}$. Proposition 1.27 (v) implies that R is contained in the intersection of the corresponding exponent rings, but this intersection equals $\mathbb{C}$, and so $\mathbb{C}(X)$ cannot be the quotient field of R, contrary to our assumption.

To begin with, we shall develop a little further the theory of valuations of arbitrary fields. Let K be a field with valuation v. This valuation induces in K the structure of a metric space which may or may not be complete. It is an elementary result in topology that every metric space can be embedded as a dense subset in a complete metric space, and this can be done in an essentially unique way. It turns out that if we do this for K, then the resulting complete metric space may be given a field structure. This is the essence of the following theorem.

Theorem 3.1. *Let K be a field with a valuation v. Then there exists a field L with a valuation w, having the following properties:*

(i) *L is complete in the topology induced by w,*

(ii) *K is a dense subset of L, and on K the valuations v and w coincide.*

Moreover, L is unique up to valuation preserving topological isomorphism, equal to the identity on K.

Proof: Let (X, d) be a complete metric space containing K as a dense subset, on which the metric d coincides with that induced by v, i.e., for $a, b \in K$ we have $d(a, b) = v(a - b)$. In particular $d(a, 0) = v(a)$. We shall give X a field structure. For $x, y \in X$ we have $x = \lim x_n$, $y = \lim y_n$ with $x_n, y_n \in K$. Observe that $v(x_n)$ tends to $d(x, 0)$, and $v(y_n)$ tends to $d(y, 0)$, thus, for some B, we have $v(x_n), v(y_n) \leq B$. Moreover

$$\begin{aligned} d(x_n + y_n, x_m + y_m) &= v(x_n + y_n - x_m - y_m) \\ &\leq v(x_n - x_m) + v(y_n - y_m) \\ &= d(x_n, x_m) + d(y_n, y_m), \end{aligned} \tag{3.1}$$

and

$$\begin{aligned} d(x_n y_n, x_m y_m) &= v(x_n y_n - x_m y_m) \\ &= v(x_n y_n + x_n y_m - x_n y_m - x_m y_m) \\ &\leq v(x_n) v(y_n - y_m) + v(y_m) v(x_n - x_m) \\ &= v(x_n) d(y_n, y_m) + v(y_m) d(x_n, x_m). \end{aligned} \tag{3.2}$$

If we now choose m and n so large as to satisfy $d(x_n, x_m) < \epsilon$ and $d(y_n, y_m) < \epsilon$, then (3.1) and (3.2) imply

$$d(x_n + y_n, x_m + y_m) < 2\epsilon, \quad d(x_n y_n, x_m y_m) < 2B\epsilon,$$

hence the sequences $x_n + y_n$, $x_n y_n$ are both fundamental, and thus have limits in X, say w and z, respectively. Define $x + y = w$ and $xy = z$. We have to show that the elements w, z do not depend on the choice of the auxiliary sequences x_n and y_n, but this is easy. In fact, if, say, $x'_n \to x$, $y'_n \to y$ and $x'_n + y'_n$ tends to w', then

$$\begin{aligned} d(w, w') &= \lim d(x_n + y_n, x'_n + y'_n) = \lim v(x_n + y_n - x'_n - y'_n) \\ &\leq \limsup(v(x'_n - x_n) + v(y_n - y'_n)) \\ &= \limsup(d(x_n, x'_n) + d(y_n, y'_n)) = 0, \end{aligned}$$

and so $w = w'$. A similar argument is applicable to z.

It is obvious that X with the just introduced addition and multiplication is a ring. To prove that it is a field let x be a non-zero element of X, let $x = \lim x_n$ with $x_n \in K$, and put $A = \lim x_n$. If $A = 0$, then $x_n \to 0$, whence $x = 0$, contrary to our assumption. Thus $A \neq 0$, hence with a constant $C > 0$

we have $v(x_n) \geq C$ for sufficiently large n. If now m, n are sufficiently large, then

$$v(x_n^{-1} - x_m^{-1}) = \frac{v(x_n - x_m)}{v(x_n)v(x_m)} \leq \frac{v(x_n - x_m)}{C^2},$$

showing that the sequence x_n^{-1} is fundamental. Denoting its limit by y we find $xy = \lim x_n x_n^{-1} = 1$, and so x has an inverse.

If for $x \in X$ w put $w(x) = d(x, 0)$, then for every sequence x_n of elements of K for which $\lim x_n = x$ we have $\lim v(x_n) = w(x)$. The function w coincides with v on K, and via the passage to the limit we obtain that w is a valuation of X. It remains to show the uniqueness of the field X, so obtained, but this is immediate by the corresponding result for completion of metric spaces, because the topological isomorphism transfers also the algebraic structure in view of the continuity of algebraic operations and the density of K in X. □

From the proof of the theorem we derive now some simple, but useful corollaries. In all of them K is a field with valuation v, L is its completion and w is the valuation of L, prolonging v. Moreover put

$$R_w = \{x \in L : \ w(x) \leq 1\}, \quad R_v = \{x \in K : \ v(x) \leq 1\}$$

and

$$P_w = \{x \in L : \ v(x) < 1\}, \quad P_v = \{x \in K : \ v(x) < 1\}.$$

Corollary 1. *Assume that the valuation v is discrete and non-trivial. Then w is also discrete, the ring R_w is the closure of R_v, and the prime ideal P_w is the closure of P_v.*

Proof : If $x \in L$ and $x_n \to x$ with $x_n \in K$, then $\lim v(x_n) = w(x)$, whence either $w(x) = 0$, in which case $x = 0$, or $v(x_n)$ is constant for sufficiently large n. This shows $v(K) = w(L)$ and all assertions of the corollary follow immediately. □

Corollary 2. *If v is discrete and the quotient R_v/P_v is finite, then the map $R_v/P_v \longrightarrow R_w/P_w$, induced by the embedding $K \longrightarrow L$ is an isomorphism.*

Proof : Since $P_v \subset P_w$, this map is an embedding, and the preceding corollary shows that its image is dense in R_w/P_w, but it is finite and so has to coincide with R_w/P_w. □

Corollary 3. *If v is Archimedean, so is w.*

Proof : This follows from Proposition 1.25, since the fields K and L have the same prime field. □

We shall need a proposition describing topologies in finite-dimensional linear spaces over a complete field K, which are consistent with the topology of K:

Proposition 3.2. *Let K be a complete field with valuation v, and let E be a finite-dimensional linear space over K. If E has a norm topology in which addition and multiplication by scalars from K are continuous, and, moreover, it is consistent with the topology of K, i.e., induces the topology of K on one-dimensional subspaces $\{ax : a \in K\}$ (with fixed non-zero $x \in E$), then this topology coincides with the product topology. This means that the mapping*

$$f : [x_1, \ldots, x_n] \mapsto \sum_{j=1}^{n} x_j a_j \quad (x_j \in K),$$

with the a_i's forming a K-basis of E, is a topological isomorphism between K^n and E.

Proof : As f is a continuous isomorphism, it remains to prove the following statement:

If $\| x \|_v$ denotes the norm on E, then for a suitable $C > 0$ we have

$$v(x_i) \leq C \| \sum_{j=1}^{n} x_j a_j \|_v$$

for $x_j \in K$.

For $r = 0, 1, \ldots, n$ denote by E_r the subset of E consisting of all x for which in $x = \sum_{j=1}^{n} x_j a_j$ at most r of the x_j's are non-zero. We prove our statement for $x \in E_r$ by induction in r. The case $x \in E_1$ being covered by the assumption, assume that our statement is true for all elements of E_{r-1} with the coefficient C_1 in place of C. If our assertion would fail for $x \in E_r$, then there would exist a an r-tuple of indices $i_1, \ldots, i_r$ and a sequence $x^{(m)} \neq 0$ with

$$x^{(m)} = x_{i_1}^{(m)} a_{i_1} + \cdots + x_{i_r}^{(m)} a_{i_r},$$

such that the quotient $\| x^{(m)} \|_v / v(x_{i_1}^{(m)})$ tends to zero. For

$$y^{(m)} = x^{(m)} / x_{i_1}^{(m)} = a_{i_1} + y_{i_2}^{(m)} a_{i_2} + \cdots + y_{i_r}^{(m)} a_{i_r}$$

we have $\| y^{(m)} \|_v \to 0$, and so $y^{(m)}$ tends to 0. But this leads to a contradiction. In fact, the differences $y^{(m)} - y^{(n)}$ all lie in E_{r-1}, and by the inductive assumption we get

$$v(y_{i_j}^{(m)} - y_{i_j}^{(n)}) \leq C_1 \| y^{(m)} - y^{(n)} \|_v \to 0$$

for $j = 2, \ldots, r$. Thus the sequences $y_{i_j}^{(m)}$ are fundamental for $j = 2, \ldots, r$. Due to the completeness of K they have limits, say $\lim y_{i_j}^{(m)} = z_j$. But then

$$\lim y^{(m)} = a_{i_1} + z_2 a_{i_2} + \cdots + z_r a_{i_r} \neq 0,$$

contradiction. □

2. Now we prove a theorem of Ostrowski, describing all valuations of algebraic number fields:

Theorem 3.3. *Let K be an algebraic number field of degree n over the rationals, and let v be a non-trivial valuation of K. Then v is either discrete or Archimedean. If v is discrete, then there is a prime ideal $\mathfrak{p}$ of R_K such that for a certain $0 < a < 1$ we have $v(x) = a^{\nu(x)}$, where ν is the exponent of $\mathfrak{p}$. If v is Archimedean, then it is equivalent to $|F(x)|$, with F being an embedding of K in $\mathbb{C}$. Conversely, every prime ideal of R_K defines in this way a valuation of K, and every embedding $K \longrightarrow \mathbb{C}$ defines an Archimedean valuation. Valuations defined by different prime ideals are non-equivalent, and two valuations defined by different embeddings of K into $\mathbb{C}$ are equivalent if and only if these embeddings are complex conjugated.*

Proof : Were v non-Archimedean and non-discrete, then the group $v(K^*)$ would be dense in the positive half-line. Let L be the completion of K with respect to v, and let w be its valuation. Now let $y \in K^*$ and let $\sum_{j=0}^{m} c_j X^j \in \mathbb{Q}[X]$ be the minimal polynomial of y over $\mathbb{Q}$. We have

$$0 = w(0) = w(\sum_{j=0}^{m} c_j y^j),$$

and since w is non-Archimedean there must be non-zero terms $c_i y^i$, $c_j y^j$ with $i \neq j$, such that $w(c_i y^i) = w(c_j y^j)$. Then

$$w(y)^{j-i} = w(c_i/c_j) = v(c_i/c_j)$$

lies in a discrete set, and in view of $|i - j| \leq [K : \mathbb{Q}]$ the same applies to $w(y)$. As $y \in K^*$ was arbitrary this shows that $v(K^*)$ cannot be dense, contradiction.

Now let v be discrete. With a suitable exponent ν and $0 < a < 1$ we have $v(x) = a^{\nu(x)}$ for all non-zero $x \in K$. Denote by μ the restriction of ν to $\mathbb{Q}$, and observe that μ does not vanish identically. In fact, if it were so, then we would have

$$\mathbb{Q} \subset R_v = \{x \in K : \ \nu(x) \geq 0\},$$

and since by Theorem 1.26 the ring R_v is Dedekind, thus integrally closed in K, it would contain the integral closure of $\mathbb{Q}$ in K, i.e. the field K, which is possible only in the case of trivial v, which we excluded. Thus $\mu \neq 0$ and if e denotes the minimal positive value attained by μ, then $\mu(x)/e$ is an exponent of $\mathbb{Q}$, which, by Theorem 1.31, is induced by a rational prime p. Hence for $x \in \mathbb{Z}$ we have $\nu(x) = \mu(x) \geq 0$, thus $\mathbb{Z} \subset R_\nu$. As R_ν is integrally closed, and R_K is the integral closure of $\mathbb{Z}$ in K, we get $R_K \subset R_\nu$.

Consider now

$$\mathfrak{p} = \{x \in R_K : \ \nu(x) > 0\} = P_\nu \cap R_K.$$

Obviously $\mathfrak{p}$ is a prime ideal of R_K and we shall show that it induces ν. Denote by γ the exponent induced by $\mathfrak{p}$, and choose x with $\gamma(x) = 0$. We may write $xR_K = I_1 I_2^{-1}$, I_1, I_2 being ideals of R_K with $(I_1 I_2, \mathfrak{p}) = 1$. Choose $a \in I_2 \setminus \mathfrak{p}$. Then $ax \in I_1 \setminus \mathfrak{p}$. Thus $\nu(a) = \nu(ax) = 0$ and $\nu(x) = 0$ follows. Therefore $\gamma(x) = 0$ implies $\nu(x) = 0$. Now fix $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ and let $x \in R_K$ be arbitrary. If $\gamma(x) = c$, then write $x\pi^{-c} = y$. Since $\gamma(y) = \nu(y) = 0$, we get $\nu(x) = \gamma(x)\nu(\pi)$. There exists $x_0 \in K$ with $\nu(x_0) = 1$, thus $1 = \gamma(x_0)\nu(\pi)$, proving $\nu(\pi) = 1$, and the equality $\nu = \gamma$ becomes obvious. The remaining assertions concerning discrete v are contained in remarks preceding Theorem 1.26.

Now let v be Archimedean. Its restriction to $\mathbb{Q}$ is also Archimedean, hence by Theorem 1.31 and Proposition 1.23 we have $v(x) = |x|^a$ for all $x \in \mathbb{Q}$ with a suitable a.

Let L be the completion of K and w let be the extension of v to L. The field L contains the closure of $\mathbb{Q}$, which is obviously topologically isomorphic to $\mathbb{R}$ with the usual topology, and which we shall identify with $\mathbb{R}$. We shall show that L, as a linear $\mathbb{R}$-space, is finite-dimensional. Choose a $\mathbb{Q}$-basis $\omega_1, \ldots, \omega_n$ of the linear space K, and let x be an arbitrary element of L. With suitable rational $a_k^{(m)}$ we have $x = \lim_m \sum_{k=1}^n a_k^{(m)} \omega_k$. Without restricting generality we may assume that the elements $\omega_1, \ldots, \omega_r$ are linearly independent over $\mathbb{R}$, whereas for $j = 1, 2, \ldots, n - r$ we have

$$\omega_{r+j} = \sum_{k=1}^{r} \lambda_k^{(j)} \omega_k$$

with real $\lambda_k^{(j)}$. Thus we may write

$$x = \lim_m \sum_{k=1}^{r} c_k^{(m)} \omega_k, \tag{3.3}$$

with real $c_k^{(m)}$.

Denote by M the $\mathbb{R}$-subspace of L spanned by $\omega_1, \ldots, \omega_r$. As it is finite-dimensional, and w serves as a norm satisfying the assumptions of Proposition 3.2, we may apply it to infer that M is closed. But (3.3) shows that M is dense in L, whence $M = L$, and we see that L has finite dimension over $\mathbb{R}$. But L is a field, and therefore we have either $L = \mathbb{R}$, or $L = \mathbb{C}$ (with the product topology). Therefore w induces the usual topology on L in both cases. If $L = \mathbb{R}$ this gives the equality $w(x) = |x|^a$ at once, whereas in the second we need some more reasoning. In this case w is continuous in the usual topology and $w(xy) = w(x)w(y)$. For $x = r\exp(it)$ with $r = |x|$ we obtain

$$w(x) = w(r)w(\exp(it)) = r^a w(\exp(it)).$$

But for $t = 2\pi p/q$ with $p, q \in \mathbb{Z}$, $q > 0$, we obtain $w(\exp(it))^q = 1$, and since such numbers $\exp(it)$ are dense on the circle $|z| = 1$, we get $w(\exp(it)) = 1$ for all t, and we obtain $w(x) = r^a = |x|^a$. In our proof we identified K with its image in the complex field. However, if we treat K in an abstract manner, and denote by $F_i(K)$ $(i = 1, 2, \ldots, n)$ its embeddings in $\mathbb{C}$, then we obtain $w(x) = |F_i(x)|^a$ for a certain i.

It remains to show that if two embeddings of K in $\mathbb{C}$ define the same valuation, then they are conjugate. This is done in the next lemma:

Lemma 3.4. *Let K be a field, and let f_1, f_2 be embeddings of K in $\mathbb{C}$ such that for all x we have $|f_1(x)| = |f_2(x)|$. Then either $f_1 = f_2$ or $f_1 = \bar{f}_2$.*

Proof : Let $a \in K$ and put $b_i = f_i(a)$ $(i = 1, 2)$. Then

$$1 + b_1 + \bar{b}_1 + b_1\bar{b}_1 = |1 + b_1|^2 = |f_1(1+a)|^2 = |f_2(1+a)|^2 = 1 + b_2 + \bar{b}_2 + b_2\bar{b}_2,$$

but $b_1\bar{b}_1 = |f_1(a)|^2 = |f_2(a)|^2 = b_2\bar{b}_2$, and we get $2\mathrm{Re}\, b_1 = b_1 + \bar{b}_1 = b_2 + \bar{b}_2 = 2\mathrm{Re}\, b_2$. Finally we see that either $b_2 = b_1$ or $b_2 = \bar{b}_1$. Now let

$$K_1 = \{a \in K : \ f_1(a) = f_2(a)\}, \quad K_2 = \{a \in K : \ f_1(a) = \overline{f_2(a)}\}.$$

Obviously K_1, K_2 are subfields of K and $K = K_1 \cup K_2$. If the K_i's are proper subfields of K, and we choose $a_1 \in K_1 \setminus K_2$ and $a_2 \in K_2 \setminus K_1$, then $a_1 + a_2$ belongs neither to K_1 nor to K_2, but lies in K, contradiction. Thus either $K = K_1$ or $K = K_2$. □

The last assertion of the theorem follows now immediately. □

Corollary. *Let K be an algebraic number field. If for a non-Archimedean valuation v we put $R_v = \{a \in K : \ v(a) \leq 1\}$, then*

$$R_K = \bigcap_v R_v,$$

the intersection taken over all non-Archimedean valuations of K.

Proof : Follows from the theorem and Proposition 1.27 (v). □

If v is an Archimedean valuation of an algebraic number field, then for simplicity we shall say that v is *real* or *complex*, if v corresponds to a real, respectively complex, embedding of K.

3. We conclude this section with the proof of a very important although simple *product formula* for valuations of algebraic number fields. To begin with we define the *normalized valuations* of K. If v is a discrete valuation of K, then the preceding theorem shows that $v(x) = a^{\nu(x)}$, where ν is the exponent induced by a prime ideal $\mathfrak{p}$ of R_K. By the Corollary to Theorem

1.20 the cardinality $N(\mathfrak{p})$ of the factor ring $R/\mathfrak{p}$ is finite. We shall say that v is normalized, if $a = N(\mathfrak{p})^{-1}$. In the case of an Archimedean valuation we consider the corresponding embedding $F : K \longrightarrow \mathbb{C}$. A real valuation v is normalized, if $v(x) = |F(x)|$, but if v is complex, then things get more complicated. We adopt the convenient convention of calling every power of a valuation also a valuation, even if it does not satisfy the triangle inequality. This convention allows us to define the normalized valuation corresponding to a non-real embedding F as $|F(x)|^2$.

Now we may state the product formula:

Theorem 3.5. *Let V be the set of all normalized valuations of an algebraic number field K. Then for every nonzero $a \in K$ we have*

$$\prod_{v \in V} v(a) = 1.$$

Proof : Let $aR_K = \prod \mathfrak{p}^{n(\mathfrak{p})}$ be the factorization of the fractional ideal generated by a into prime ideals. Since only finitely many exponents $n(\mathfrak{p})$ are non-zero, we see that only finitely many terms in our product are $\neq 1$. If $v_\mathfrak{p}$ denotes the normalized valuation associated with the prime ideal $\mathfrak{p}$, then $v_\mathfrak{p}(a) = N(\mathfrak{p})^{-n(\mathfrak{p})}$, thus the product $\prod v(a)$ extended over all discrete valuations equals $N(aR_K)^{-1}$. On the other hand, this product extended over all Archimedean valuations equals $|N_{K/\mathbb{Q}}(a)|$, and the Corollary to Proposition 2.13 can now be used to complete the proof. □

3.2. Ideal Classes

1. Since the ring R_K is a Dedekind domain, we may consider the group of its ideal classes, as defined in Chap. 1. Recall that this group consists of isomorphism classes of ideals of R_K, considered as R_K-modules, with multiplication induced by the usual ideal multiplication. The fact that this multiplication induces a group structure was established in Proposition 1.43. It is customary to denote the resulting group by $H(K)$ and call it the *class-group of K*. The case $m = n = 1$ of Theorem 1.39 shows that $H(K)$ is isomorphic to the quotient group $G(K)/P(K)$, where $G(K)$ is the group of all fractional ideals of K, and $P(K)$ is its subgroup consisting of principal fractional ideals. One of the principal aims of this section is to prove that $H(K)$ is finite. Actually we shall consider also some generalizations of the class group, and prove finiteness for this more general family of groups.

Denote by $D(K)$ the product of the group $G(K)$ and the signature group $Sgn(K)$, as defined in Chap. 2. Denote by $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r_1,\infty}$ the generators of $Sgn(K)$, and consider the homomorphism f of the multiplicative group K^* of K into $D(K)$, defined by

$$f(a) = \mathfrak{p}_{1,\infty}^{\epsilon_1} \cdots \mathfrak{p}_{r_1,\infty}^{\epsilon_{r_1}} \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})},$$

where $\epsilon_i \in \{0,1\}$ are defined by $\operatorname{sgn} F_i(a) = (-1)^{\epsilon_i}$, and $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ is the factorization into prime ideals of the ideal aR_K.

The group $D(K)$ is called the *divisor group* of K, the elements $\mathfrak{p}_{i,\infty}$ are called the *real infinite prime divisors*, and the elements of the subgroup of $D(K)$, generated by prime ideals are called the *finite divisors*. The image $f(K^*)$ is the group of *principal divisors*, and its projection on $G(K)$, which is clearly isomorphic with $P(K)$, is the *group of finite principal divisors*. Finally, the intersection $f(K^*) \cap G(K)$ is called the *group of positive principal divisors* and is denoted by $P_+(K)$.

The quotient group $G(K)/P(K)$ equals $H(K)$, but the quotient group $G(K)/P_+(K)$ is generally larger. It is called the *narrow class group* and is denoted by $H^*(K)$. Both are of utmost importance in the study of multiplicative properties of R_K.

The classical definition of those groups (equivalent to the given above) runs as follows: two ideals I,J of R_K are called *equivalent* if for some non-zero $a, b \in R_K$ we have $aI = bJ$. The ideals I, J are *equivalent in the narrow sense*, if this equality holds with some totally positive $a, b \in R_K$. The set of all equivalence classes in the first sense, with multiplication induced by multiplication of ideals forms $H(K)$, whereas the second kind of equivalence leads to $H^*(K)$. The proof of the equivalence of the two definitions follows easily from Proposition 1.43.

Now we make another generalization. Let I be any non-zero ideal of R_K, and consider the group A_I of all elements $x \in K^*$ which are representable in the form $x = ab^{-1}$ with $a, b \in R_K$, $a \equiv b \pmod{I}$, and $(abR_K, I) = 1$. Moreover, let $G_I(K)$ be the group of all fractional ideals of K which are quotients of two ideals prime to I, and let $P_I(K)$ be the subgroup of $G_I(K)$ consisting of principal fractional ideals generated by elements of A_I. We consider $G_I(K)$ as a subgroup of $D(K)$ through the embeddings $G_I(K) \subset G(K) \subset D(K)$. Finally, denote by $P_I^+(K)$ the subgroup of $P_I(K)$, consisting of fractional ideals having totally positive generators. The quotient group $H_I(K) = G_I(K)/P_I(K)$ is called the *group of ray classes* mod I, and $H_I^*(K) = G_I(K)/P_I(K)^+$ is called the *group of narrow ray classes* mod I. Note that for $I = R_K$ we obtain $H_I(K) = H(K)$ and $H_I^*(K) = H^*(K)$. One may also give an equivalent definition, considering two ideals A, B, prime to I, as equivalent mod I, if with suitable $a, b \in R_K$ congruent to 1 mod I we have $aA = bB$, and the narrow equivalence is defined analogously with the additional requirement for a, b to be totally positive. In future, speaking about ideal classes mod I, we shall always have the last interpretation in mind.

2. Now we are going to prove the finiteness of all groups introduced in the preceding subsection. To begin with, we show that it is enough to prove this result for the group $H(K)$.

Lemma 3.6. *Let I be a non-zero ideal of R_K. The homomorphism $\psi : H_I^*(K) \longrightarrow H(K)$ induced by the embedding $G_I(K) \subset G(K)$ has a finite kernel, and so if $H(K)$ is finite, then $H_I^*(K)$ is finite as well.*

Proof : The kernel of ψ consists of all classes mod I in the narrow sense which contain a principal ideal, and so equals the quotient of the group of all principal fractional ideals prime to I by the group of all ideals generated by a totally positive element of the form a/b with $a, b \in R_K$ and $a \equiv b \equiv 1 \,(\mathrm{mod}\, I)$. Every coset of this quotient group contains a principal ideal generated by an integer. Indeed, if $ab^{-1}R_K$ is a principal fractional ideal with $a, b \in R_K$, relatively prime to I, then $c = b^{2\Phi(I)}$ is totally positive and congruent to unity mod I by Theorem 1.19. Thus $ab^{-1}R_K$ and $ab^{2\Phi(I)-1} = ab^{-1}cR_K$ are in the same coset. Therefore it suffices to prove the existence of a finite set of integers $a_1, \ldots, a_r$ in R_K, such that every integer $x \in R_K$, prime to I, becomes totally positive and congruent to 1 mod I after multiplication by one of the a_i's. This can be done by choosing from every fixed residue class mod I a set of elements representing all signatures, which is possible by Proposition 2.2 (i). Since there are 2^{r_1} different signatures and $\Phi(I)$ different residue classes, the set so constructed is finite, and clearly has the required property. □

Theorem 3.7. *For every non-zero ideal I of R_K the groups $H_I(K)$ and $H_I^*(K)$ are finite.*

Proof : By Lemma 3.6 it suffices to prove the theorem for the group $H(K)$. The proof is based on a lemma:

Lemma 3.8. *If K is of degree n over the rationals and has signature $[r_1, r_2]$, then in every ideal class there exists an ideal $I \subset R_K$ with*

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d(K)|}.$$

Proof : Let X be a class in $H(K)$ containing $I \subset R_K$. By Proposition 1.43 there is an ideal $J \subset R_K$ belonging to the class X^{-1}, and therefore $IJ = aR_K$ is principal. Since the index of J in R_K equals $N(J)$, we may use Lemma 2.23 to obtain $c \neq 0$ in J with

$$|N_{K/\mathbb{Q}}(c)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d(K)|} N(J).$$

The ideal cR_K is divisible by J, hence we have $A = cJ^{-1} \subset R_K$, and the ideals I and A are equivalent, thus $A \in X$. But

$$N(A) = |N_{K/\mathbb{Q}}(c)|/N(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(K)|}$$

by Corollary to Proposition 2.13. □

The theorem follows now from Theorem 1.16 (ii).

The number of elements in $H(K)$, $H^*(K)$, $H_I(K)$ and $H_I^*(K)$ are denoted by $h(K)$, $h^*(K)$, $h_I(K)$ and $h_I^*(K)$, respectively. We shall call these numbers the *class number*, *narrow class number*, *class number* mod I, and *narrow class number* mod I, respectively. The presented proof of Theorem 3.7 shows that $h(K)$ cannot exceed the number of ideals of R_K whose norms do not exceed the number

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(K)|},$$

which is called the *Minkowski constant of the field* K.

This implies, for example, that quadratic fields with discriminants $d(K) = -3, -4, -7, -8, 5, 8, 12$ and 13 as well as cubic fields with $-49 \leq d(K) < 81$ have $h(K) = 1$, since in these cases only the trivial ideal has its norm bounded by the Minkowski constant. Theorem 1.45 implies that the rings of integers of these fields are unique factorization domains.

We point out two corollaries to Theorem 3.7:

Corollary 1. *If I is a fractional ideal in K, then $I^{h(K)}$ is principal.* □

Corollary 2. *If I is a fractional ideal in K and for a certain positive m the ideal I^m is principal, then either I is principal itself, or $(m, h(K)) \neq 1$.* □

The determination of the structure of class groups is one of the main goals of the theory of algebraic numbers. In the next section the reader will find some results connecting $h_I^*(K)$ with $h(K)$, so that the problem of determination of $h_I^*(K)$ will be reduced to the simplest case.

Now we present an example of a field with class number bigger than 1, i.e. whose ring of integers is not a unique factorization domain. Consider $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt{-5}$ and the ideal $I = 2R_K + (1+\theta)R_K$. We have $N(I)|N(2R_K) = 4$ and $N(I)|N(1+\theta) = 6$, thus $N(I)$ equals either 1 or 2. If $N(I) = 1$, then $I = R_K$ and for some $x, y \in R_K$ we have $1 = 2x + (1+\theta)y$. Write $x = a + b\theta$, $y = c + d\theta$ with $a, b, c, d \in \mathbb{Z}$, which is possible by Theorem 2.18. This leads to

$$1 = (2a + c - 5d) + (2b + d + c)\theta,$$

thus $2a + c - 5d = 1$, $2b + d + c = 0$. But this system has no integral solutions, since it implies that $c + d$ is at the same time even and odd, which is absurd. Hence $N(I) = 2$. To prove $h(K) \neq 1$ we have to show that there is no principal ideal of norm 2, i.e., there is no $a \in R_K$ with $N_{K/\mathbb{Q}}(a) = 2$ (obviously, there cannot exist elements of norm -2, since K is quadratic imaginary), but this is achieved by the observation that for $x, y \in \mathbb{Z}$ we have $N_{K/\mathbb{Q}}(x + y\theta) = x^2 + 5y^2 \neq 2$.

3.3. Units

1. This section is devoted to *units*, i.e., invertible elements of the ring of all algebraic integers. As in every domain, the units form a group under multiplication. Units lying in a fixed algebraic number field K form a subgroup of that group; we shall denote it by $U(K)$. Its elements will be called *units of the field* K, which is perhaps not the best name, since they are in fact units of R_K, every non-zero element of K being invertible in K.

We shall determine the structure of the group $U(K)$; this was first done by Dirichlet in 1840 in a slightly different setting, since his definition of an algebraic integer does not coincide with the one used now.

We shall also consider divisibility in R_K. We say that a divides b and write $a|b$ if a, b and the quotient b/a are integers. Note that this definition does not depend on the field in which a, b are contained. If $a|b$ and $b|a$, then we say that a and b are *associated*. Obviously, this happens if and only if the quotient b/a is a unit, and this means, that the principal ideals generated by a and b in any ring R_K containing these numbers coincide. The following easy result will be used quite often:

Proposition 3.9. *If $a, b \in R_K$ and $a|b$, then $N_{K/\mathbb{Q}}(a)$ divides $N_{K/\mathbb{Q}}(b)$.*

Proof : Apply Proposition 2.4 (i) to the equality $b = a(ba^{-1})$. □

Now we prove some elementary results concerning units.

Proposition 3.10. *If a is an algebraic integer, then the following conditions are equivalent:*

(i) *a is a unit,*

(ii) *$a|1$,*

(iii) *For every field K containing a, $|N_{K/\mathbb{Q}}(a)| = 1$,*

(iv) *There is a field K containing a such that $|N_{K/\mathbb{Q}}(a)| = 1$,*

(v) *There is a monic polynomial $F \in \mathbb{Z}[X]$ with $F(a) = 0$ and $|F(0)| = 1$.*

(vi) *There is a polynomial $G(X) = \sum_{j=0}^{n} c_j X^j$ with integral coefficients, such that c_0 and c_n are units and $G(a) = 0$.*

Proof : The implications (i) $\Rightarrow$ (ii), (iii) $\Rightarrow$ (iv) and (v) $\Rightarrow$ (vi) are trivial and (ii) $\Rightarrow$ (iii) follows from the preceding proposition. To prove (iv) $\Rightarrow$ (v) take for F the minimal polynomial for a over $\mathbb{Z}$, and observe that $N_{K/\mathbb{Q}}(a)$ equals some power of $\pm F(0)$. Finally, to establish (vi) $\Rightarrow$ (i) observe that the polynomial $W(X) = c_0^{-1} X^n G(X^{-1})$ has integral coefficients, is monic and vanishes at a^{-1}, thus a^{-1} is integral over the field generated by the coefficients of G. By Theorem 1.7 a^{-1} is integral over $\mathbb{Z}$ and thus a is a unit. □

Evidently roots of unity lying in K form the maximal torsion subgroup of $U(K)$, which we shall denote by $E(K)$.

Proposition 3.11. *The group $E(K)$ is a finite cyclic group whose order is even and divides $2d(K)$.*

Proof : If $\zeta \neq 1$ lies in $E(K)$, then we can write

$$\zeta = \prod_{i=1}^{s} \zeta_{q_i}^{n_i},$$

where $q_i = p_i^{m_i}$ are powers of distinct primes p_i and n_i are positive rational integers satisfying $p_i \nmid n_i$. Put $q = \max q_i$ and $N = \left(\prod_{i=1}^{s} q_i\right)/q$. The number ζ^N lies in K and is a primitive qth root of unity. If $q = p^a$, then the degree of ζ^N equals $p^{a-1}(p-1)$ by Theorem 2.20, hence $p^{a-1}(p-1) \leq [K : \mathbb{Q}]$, and we get only finitely many possibilities for q. In view of $q_i \leq q$, the same applies to q_i. This shows that $E(K)$ is finite, and so it must be cyclic, since every finite subgroup of the group of all roots of unity is cyclic. Its order is even, because it contains the subgroup $\{1, -1\}$. To prove the last assertion factorize $\#E(K)$ into primes:

$$\#E(K) = \prod p_i^{n_i}.$$

The fields $\mathbb{Q}(\zeta_{p_i^{n_i}})$ are subfields of K, and so, by Proposition 2.16 their discriminants divide $d(K)$. But, by Theorem 2.20 they are equal to $\pm p_i^{A_i}$ with

$$A_i \geq B_i = \begin{cases} n_i & \text{if } p_i \neq 2, \\ n_i - 1 & \text{if } p_i = 2, \end{cases}$$

and as $\prod p_i^{B_i}$ divides $d(K)$, the assertion follows. □

2. We prove now Dirichlet's unit theorem in the form due to Chevalley and Hasse. To state it we need certain definitions.

Let S be a finite set of non-equivalent normalized valuations of K containing the set S_∞ of all Archimedean valuations. A non-zero element $a \in K$ is called *S-integral*, resp. an *S-unit*, if for every valuation $v \notin S$ we have $v(a) \leq 1$, resp. $v(a) = 1$. Note that if $S = S_\infty$, then S-integral elements

are exactly the integers of K, and S-units coincide with algebraic units, defined in the preceding subsection. The first assertion is a reformulation of the Corollary to Theorem 3.3, and the second follows now by the observation that for $a \in K^*$ the equality $v(a) = 1$ is equivalent to $v(a), v(a^{-1}) \leq 1$.

It is not difficult to see that the ring K_S of S-integers is a Dedekind ring. The S-units are invertible elements of K_S, and therefore form a group $U_S(K)$ under multiplication.

Theorem 3.12. (The Dirichlet-Chevalley-Hasse theorem) *The group $U_S(K)$ is the direct product of the group of roots of unity $E(K)$ and a free Abelian group with $s-1$ free generators, s being equal to the number of elements in S.*

The special case $S = S_\infty$ gives the celebrated Dirichlet unit theorem:

Theorem 3.13. *The group $U(K)$ is the direct product of the group of roots of unity $E(K)$ and a free Abelian group with $r = r_1(K) + r_2(K) - 1$ free generators.*

Proof of Theorem 3.12. The idea of the proof is very simple. One constructs a homomorphism of $U_S(K)$ into the real s-space, whose kernel equals $E(K)$, and then one proves that the image of $U_S(K)$ is a $(s-1)$-dimensional lattice, i.e., a free Abelian group with $s-1$ free generators. Since by Corollary to Proposition 1.33 every free $\mathbb{Z}$-module is projective (and an Abelian group and a $\mathbb{Z}$-module means the same), Proposition 1.34 (i) shows that $U_S(K)$ has the asserted form.

Thus consider the mapping $\Phi : U_S(K) \longrightarrow \mathbb{R}^s$ given by

$$\Phi : x \mapsto [\log v(x)]_{v \in S}.$$

At our first step we prove that $\Phi(U_S(K))$ is a lattice:

Lemma 3.14. *The image $\Phi(U_S(K))$ is a discrete subgroup of $\mathbb{R}^s$.*

Proof : Since Φ is a homomorphism, the image of $U_S(K)$ is a subgroup of $\mathbb{R}^s$. Therefore it suffices to show that there is a neighbourhood of zero containing only finitely many elements of $\Phi(U_S(K))$. Assume the contrary. Then there exist infinitely many $x \in U_S(K)$ such that for Archimedean v we have $|\log v(x)| < 1$, and for non-Archimedean $v = v_\mathfrak{p} \in S$ (where $\mathfrak{p}$ is the corresponding prime ideal in R_K) we have $|\log v_\mathfrak{p}(x)| < \log N(\mathfrak{p})$. If $c_\mathfrak{p}$ is the exponent corresponding to $\mathfrak{p}$, then $v_\mathfrak{p}(x) = N(\mathfrak{p})^{-c_\mathfrak{p}(x)}$, and so $\log v_\mathfrak{p}(x) = -c_\mathfrak{p}(x) \log N(\mathfrak{p})$, showing that for our choice of x we have $|c_\mathfrak{p}(x)| < 1$. Since $c_p(x)$ is a rational integer, it must be zero, thus $x \in R_K$. Moreover all conjugates of x are bounded by $\exp 1$, whence we can have at most a finite number of x, contrary to our assumption. □

Observe now that Theorem 2.5 (i) implies that the kernel of Φ coincides with $E(K)$, and note that the image of $U_S(K)$ is a k-dimensional lattice with $k \leq s-1$, since, in view of Theorem 3.5, it lies entirely in the $(s-1)$-dimensional hyperplane $\sum_{j=1}^{s} X_j = 0$.

In our next step we show that the dimension of $\Phi(U_S(K))$ equals $s-1$. We shall do this first in the simplest case, when $S = S_\infty$, in which case $U_S(K) = U(K)$, and then use the finiteness of the class-group $H(K)$ to treat the general case.

Let $n = [K : Q]$, let $\omega_1, \ldots, \omega_n$ be a fixed integral basis of K, denote by I the set of all elements of K of the form $\sum_{j=1}^{n} c_j \omega_j$, where $|c_j| \leq 1$, $c_j \in Q$ $(j = 1, \ldots, n)$, and put

$$g = \max\{1, \max\{v(x) : \ x \in I, v \in S_\infty\}\}.$$

Lemma 3.15. *Let B be a positive integer. For every $a \in K$, satisfying $|N_{K/\mathbb{Q}}(a)| \leq B^n$ there exists a non-zero element b of R_K such that for $v \in S_\infty$ we have*

$$v(ab) \leq \begin{cases} gB & \text{if } v \text{ is real,} \\ gB^2 & \text{otherwise.} \end{cases}$$

Proof : Assume first $a \in R_K$. In this case the numbers

$$\sum_{j=1}^{n} c_j \omega_j \quad (0 \leq c_j \leq B, c_j \in \mathbb{Z})$$

cannot be all distinct mod aR_K, since there are $(1+B)^n > |N_{K/\mathbb{Q}}(a)| = N(aR_K)$ of them. Hence one of their non-zero differences must be divisible by a, and if we denote it by ab, then our demands will be fulfilled. If a is not integral, then write $a = a_0/m$ with $a_0 \in R_K$ and natural m. Obviously $|N_{K/\mathbb{Q}}(a_0)| \leq (mB)^n$, and so the preceding argument shows the existence of $b \in R_K$ with $v(a_0 b) \leq gmB$ and $v(a_0 b) \leq g(mB)^2$, respectively, and therefore the asserted inequalities hold for $v(ab)$. □

Corollary. *There exists a constant $M > 1$ with the property that for all $a \in K$, satisfying $1/2 < |N_{K/\mathbb{Q}}(a)| < 1$, there exists a unit $u \in U(K)$ such that $\overline{|ua|} \leq M$.*

Proof : Applying the lemma with $B = 1$ we obtain the existence of a non-zero $b = b(a) \in R_K$, satisfying $v(ab) \leq g$ for all $v \in S_\infty$. This implies $|N_{K/\mathbb{Q}}(b)| \leq 2g^n$. Theorem 1.16 (ii) shows now that the numbers $b(a)$ generate only a finite number of distinct ideals, and so there exists a finite set, say $\{b_1, \ldots, b_N\}$ such that for every a, satisfying our conditions, we have $b(a) = ub_j$ for a certain $j \leq N$ and a suitable unit u. Thus for every $v \in S_\infty$ we have

$$v(ua) = v(ab)v(ub^{-1}) = v(ab)v(b_j^{-1}) \leq M$$

for a certain constant M, which does not depend on a. □

Lemma 3.16. *If $s = r_1 + r_2 > 1$, then there exist $r = s - 1$ units in $U(K)$, whose images in $\mathbb{R}^s$ under Φ are linearly independent.*

Proof : Let $v_1, \ldots, v_s$ be all Archimedean valuations of K ordered so that $v_1, \ldots, v_{r_1}$ are real. Moreover let $0 < a_i < b_i$ $(i = 1, 2, \ldots, s)$ be given. We claim that there exists $a \in K$ with $a_i < v_i(a) < b_i$ for all i. In fact, define

$$A_i = \begin{cases} a_i & \text{for } i = 1, 2, \ldots, r_1, \\ \sqrt{a_i} & \text{for } i = r_1 + 1, \ldots, s, \end{cases}$$

and

$$B_i = \begin{cases} b_i & \text{for } i = 1, 2, \ldots, r_1, \\ \sqrt{b_i} & \text{for } i = r_1 + 1, \ldots, s. \end{cases}$$

Then our conditions take the form $A_i < |F_i(a)| < B_i$ $(i = 1, 2, \ldots, s)$, where F_i is the embedding corresponding to v_i. Now let $\omega_1, \ldots, \omega_n$ be an integral basis of K, and consider the following system of linear equations:

$$\sum_{j=1}^{n} x_j F_i(\omega_j) = h_i \quad (i = 1, 2, \ldots, n),$$

where for $i = s+1, \ldots, n$ the embeddings F_i are defined by $F_i = \overline{F_{i-r_2}}$, and h_i are real numbers, satisfying $A_i < h_i < B_i$ for $i = 1, 2, \ldots, s$ and $h_i = h_{i-r_2}$ for $i > s$. By Cramer's rule this system has a real solution $x_1, \ldots, x_n$. If we now choose rational numbers y_i, sufficiently close to x_i, so that the inequalities

$$A_i < |\sum_{j=1}^{n} y_j F_i(\omega_j)| < B_i \quad (i = 1, 2, \ldots, s)$$

hold (where for $i > s$ we put $A_i = A_{i-r_2}$ and $B_i = B_{i-r_2}$), then the number $a = \sum_{j=1}^{n} y_j \omega_j$ gives what is required.

This being done, we can now find $a_1, \ldots, a_s \in K$, satisfying the inequalities

$$M < v_i(a_j) < cM \quad (i \neq j),$$

$$\frac{1}{2M^r} < v_j(a_j) < \frac{1}{(cM)^r},$$

where the constant $c > 1$ satisfies $1 < c < 2^{1/r}$. Then we get $1/2 < |N_{K/\mathbb{Q}}(a_i)| < 1$, and by Corollary to Lemma 3.15 we obtain for suitable units u_i the inequality $v_j(u_i a_i) < M$ for all j. In particular for $i \neq j$ we get $v_j(u_i) < 1$, i.e., $\log v_j(u_i) < 0$. Now consider the matrix $[\log v_j(u_i)]$ with $1 \leq i, j \leq r$. We have to show that it is non-singular. For this purpose note that the product formula (Theorem 3.5) gives

$$\sum_{j=1}^{r} \log v_j(u_i) = -\log v_s(u_i) > 0 \quad (i = 1, 2, \ldots, r),$$

and so our assertion follows from the observation that is $[a_{ij}]$ is a $n \times n$ real matrix with $a_{ij} < 0$ for $i \neq j$ and $\sum_{j=1}^{n} a_{ij} > 0$, then its determinant does not vanish. Indeed, otherwise there would exist a system $x_1, \ldots, x_n$ of real numbers, not all equal to zero, and such that

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \quad (i = 1, 2, \ldots, n).$$

We may assume that $\max |x_j| = x_N$, changing signs, if necessary, of all numbers x_i, and then we obtain a clear contradiction:

$$0 = \sum_{j=1}^{n} a_{Nj} x_j = a_{NN} x_N + \sum_{j \neq N} a_{Nj} x_j \geq x_N \sum_{j=1}^{n} a_{Nj} > 0.$$

Therefore the dimension of $\Phi(U(K))$ equals r. □

Now we come back to the general situation:

Lemma 3.17. *There exist $s - 1$ units in $U_S(K)$, whose images in R^s are linearly independent.*

Proof : Since $U(K) \subset U_S(K)$, we may consider $\Phi(U(K))$ as a sublattice of $\Phi(U_S(K))$. Moreover $\Phi(U(K)) \sim U(K)/E(K)$, $\Phi(U_S(K)) \sim U_S(K)/E(K)$, thus $\Phi(U_S(K))/\Phi(U(K)) \sim U_S(K)/U(K)$ is a free Abelian group with at most $s - 1 - r = s - r_1 - r_2 = m$ free generators by Lemma 3.16. We have to prove that it has exactly m free generators. In order to do this it suffices to show the existence of m multiplicatively independent elements in that group, i.e., elements for which no product of their integral powers can be equal to the unit element, except the trivial case, when all exponents are zero. Let $v_1, \ldots, v_m$ be the discrete valuations in S and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ be the corresponding prime ideals of R_K. The ideals $\mathfrak{P}_i^{h(K)}$ are principal by Corollary 1 to Theorem 3.7, and thus have the form $a_i R_K$, where the a_i's are S-units. We claim that their images are multiplicatively independent in $U_S(K)/U(K)$. In fact, if for some rational integers $t_1, \ldots, t_m$ we have $a = \prod_i a_i^{t_i} \in U(K)$, then the ideal $aR_K = (\prod_i \mathfrak{P}_i^{t_i})^{h(K)}$ equals R_K, and thus Theorem 1.12 implies the vanishing of $t_1, \ldots, t_m$. □

As already said, the last lemma implies the theorem, because we have now an exact sequence

$$0 \longrightarrow E(K) \longrightarrow U_S(K) \longrightarrow \Phi(U_S(K)) \longrightarrow 0.$$

with a free (thus projective) last non-zero term. Proposition 1.34 now gives

$$U_S(K) \sim E(K) \oplus \Phi(U_S(K)),$$

and the second summand is a free Abelian group with $s-1$ free generators. □

Corollary 1. *There exist S-units $\epsilon_1, \ldots, \epsilon_{s-1}$ such that every S-unit u can be written in a unique way in the form*

$$u = \zeta \epsilon_1^{n_1} \cdots \epsilon_{s-1}^{n_{s-1}},$$

where $\zeta \in E(K)$ and $n_1, \ldots, n_{s-1} \in \mathbb{Z}$. □

Every system $\epsilon_1, \ldots, \epsilon_{s-1}$ of S-units, having the property stated in that corollary is called a *fundamental system of S-units*. In the case $S = S_\infty$ we speak simply about *fundamental system units of K*.

For any system $u_1, \ldots, u_r$ of units of K (with $r = r_1 + r_2 - 1$) we define the *regulator* $R(u_1, \ldots, u_r)$ as the absolute value of the determinant of the matrix $[\log v_j(u_i)]$, where v_j runs over all valuations from S_∞ except one.

Corollary 2. (i) *The value of the regulator does not depend on the deleted valuation.*

(ii) *The regulator $R(u_1, \ldots, u_r)$ vanishes if and only if the units u_i are multiplicatively dependent.*

(iii) *If $u_1, \ldots, u_r$ and $s_1, \ldots, s_r$ are two fundamental systems of units of K, then*

$$R(u_1, \ldots, u_r) = R(s_1, \ldots, s_r).$$

If we denote this common value by $R(K)$, and $a_1, \ldots, a_r$ is an arbitrary system of multiplicatively independent units of K, then

$$R(K) \leq R(a_1, \ldots, a_r).$$

Proof : All assertions follow from the definition of the regulator, elementary properties of determinants, and the equality $\sum_{v \in S_\infty} \log v(a) = 0$, valid for $a \in U(K)$. □

The number $R(K)$ is called the *regulator* of the field K, and $r(K) = r_1(K) + r_2(K) - 1$ is called the *unit rank of K*. If $r(K) = 0$ then we put $R(K) = 1$.

3. We shall now consider, as an example, units of quadratic fields.

Proposition 3.18. *Let $K = \mathbb{Q}(\sqrt{D})$, where $D \neq 1$ is a rational square-free integer.*

(i) *if $D < 0$, then*

$$U(K) = E(K) = \begin{cases} \{\pm 1, \pm i\} & \text{if } D = -1, \\ \{\pm 1, (\pm 1 \pm \sqrt{-3})/2\} & \text{if } D = -3, \\ \{\pm 1\} & \text{if } D \neq -1, -3. \end{cases}$$

(ii) *If $D > 0$, then there exists a unit η such that $U(K) = \{\pm \eta^n : n \in \mathbb{Z}\}$. There are four choices for η: if ϵ is one of them, then the others are $-\epsilon$, $1/\epsilon$ and $-1/\epsilon$. For one of these choices we have $\eta = (a + b\sqrt{D})/2 > 1$ with $a, b \in \mathbb{Z}$ and $a, b > 0$.*

(iii) *If $D > 0$ and the pair $< A, B >$ is a positive solution of*

$$X^2 - DY^2 = \pm 4 \tag{3.4}$$

satisfying

$$\begin{cases} A \equiv B \pmod 2 & \text{if } D \equiv 1 \pmod 4, \\ 2|A, 2|B & \text{if } D \not\equiv 1 \pmod 4, \end{cases}$$

and with minimal value of A, then $\eta = (A + B\sqrt{D})/2$.

Proof : (i) In this case we have $r(K) = 0$, and so Theorem 3.13 shows that $U(K)$ coincides with $E(K)$, Let ζ_n be a generator of $E(K)$, and let p^k be a prime power divisor of n. Then $\zeta_{p^k} \in K$ and using Theorem 2.20 we obtain $p^{k-1}(p-1) = \varphi(p^k) \leq 2$, which implies $p^k \in \{2, 3, 4\}$. Therefore $n \in \{2, 3, 4, 6, 12\}$. Since $\zeta_3, \zeta_6 \in \mathbb{Q}(\sqrt{-3})$, and $\zeta_4 = i \in \mathbb{Q}(i)$ it remains to observe that in view of

$$X^{12} - 1 = (X^2 - 1)(X^2 + 1)(X^2 + X + 1)(X^2 - X + 1)(X^4 - X^2 + 1)$$

the number ζ_{12} is a root of the irreducible polynomial $X^4 - X^2 + 1$, hence its degree equals 4.

(ii) The first assertion is a direct consequence of Theorem 3.13, since we have $r(K) = 1$ in this case, and the second follows immediately. It remains to show that if $\eta = (a + b\sqrt{D})/2 > 1$, then a and b are positive. To obtain this observe first that the sets $\{\eta, -\eta, 1/\eta, -1/\eta\}$ and $\{(\pm a \pm b\sqrt{D})/2\}$ coincide, and note that exactly one element of them has its both coefficients x, y in the canonical representation $(x + y\sqrt{D})/2$ positive. It is clear that element exceeds 1.

(iii) Let $A, B > 0$ be a positive solution of (3.4), satisfying the above congruences and with minimal A (its existence being assured by the theory of the Pellian equation), and write $\epsilon = (A + B\sqrt{D})/2$. Since $N_{K/\mathbb{Q}}(\epsilon) = (A^2 - B^2 D)/4 = \pm 1$, we have $\epsilon \in U(K)$. If $\eta > 1$ is as in (ii), then $\epsilon = \eta^n$

for a certain $n \geq 1$, since $\epsilon > 1$. We are going to show that $n = 1$. Write $\eta = (a + b\sqrt{D})/2$ with a, b positive.

Assume $n > 1$ and observe first that $B < b$, because otherwise we would have

$$a^2 = \pm 4 + Db^2 \leq \pm 4 + DB^2 = A^2,$$

contradiction.

Now

$$\frac{A + B\sqrt{D}}{2} = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k (\sqrt{D})^k$$

and

$$A = \frac{1}{2^{n-1}} \sum_{2|k} \binom{n}{k} a^{n-k} b^k D^{k/2},$$

$$B = \frac{1}{2^{n-1}} \sum_{2\nmid k} \binom{n}{k} a^{n-k} b^k D^{(k-1)/2}.$$

This implies

$$a \geq A > \frac{1}{2^{n-1}} \sum_{2|k} \binom{n}{k} a^{n-k} b^k,$$

$$b \geq B > \frac{1}{2^{n-1}} \sum_{2\nmid k} \binom{n}{k} a^{n-k} b^k,$$

and adding we get

$$a + b > \frac{1}{2^{n-1}} (a + b)^n.$$

Finally we obtain $2^{n-1} > (a + b)^{n-1}$ and $2 \leq a + b < 2$, a contradiction. □

Using this proposition and some facts from the elementary theory of numbers we are now able to find the fundamental unit of any real quadratic field.

Theorem 3.19. *Let $D > 0$ be a square-free rational integer and let $K = \mathbb{Q}(\sqrt{D})$. Denote by $\eta > 1$ the fundamental unit of K, let s be the period of the continued fraction for $\sqrt{D}$, and let P/Q be the $(s-1)$-st convergent of it. If $D \not\equiv 5 \pmod 8$, then $\eta = P + Q\sqrt{D}$, and if $D \equiv 5 \pmod 8$, then either η or η^3 equals $P + Q\sqrt{D}$. Moreover, the norm of η is positive if and only if the period s is even.*

Proof : We have to use some results from the theory of the Pellian equation, as presented for example in Sierpiński [64,p.307]. Namely, we use the following theorem:

If the period s is even, then the equation $X^2 - DY^2 = -1$ has no solutions and the smallest natural solution of $X^2 - DY^2 = 1$ is given by $X = P, Y = Q$,

whereas if s is odd, then $X = P$, $Y = Q$ is the smallest natural solution of $X^2 - DY^2 = -1$.

Observe that if $D \not\equiv 5 \pmod 8$, then every unit of K has the form $x+y\sqrt{D}$ with $x, y \in \mathbb{Z}$. In fact, if $D \not\equiv 1 \pmod 4$, then this results from the form of the integral basis given in Theorem 2.18, and in the case $D \equiv 1 \pmod 8$ one should note that if $(x+y\sqrt{D})/2$ (with $x, y \in \mathbb{Z}$) is a unit, then $x^2 - Dy^2 = \pm 4$, whence $x^2 - y^2 \equiv 4 \pmod 8$, which is possible only if x and y are both even. This remark together with the last proposition settles the case $D \not\equiv 5 \pmod 8$.

Now turn to $D \equiv 5 \pmod 8$. The number $\epsilon = (2P + 2Q\sqrt{D})/2$ is the least unit exceeding 1 for which both the coefficients in its numerator are even. This is guaranteed by the above result about Pell's equation. If ϵ is the fundamental unit, our case is settled. Otherwise we have $\epsilon = \eta^n$ for a certain $n \geq 2$, with $\eta > 1$ being the fundamental unit. If $\eta = (A + B\sqrt{D})/2$, then A and B are odd. Note now that in

$$\eta^2 = \frac{(A^2 + DB^2)/2 + AB\sqrt{D}}{2}$$

the coefficients in the numerator are both odd, but in a similar expression for η^3 they are both even, and we get $\epsilon = \eta^3$. Since the norms of ϵ and η coincide, this proves the theorem. □

This theorem gives a method of finding a fundamental unit which is not very practicable, since it involves the computation of the full period of the continued fraction of $\sqrt{D}$, which may be sometimes very long.

4. Using Dirichlet's theorem, we give now a description of fields which have a proper subfield with the same unit rank. We shall use the notation K^+ for the maximal real subfield of a field K, i.e., $K^+ = K \cap \mathbb{R}$.

Proposition 3.20. *If K is a proper subfield of L, then the groups $U(L)/E(L)$ and $U(K)/E(K)$ are isomorphic if and only if K is totally real, L is totally complex and $[L : K] = 2$. If this happens, then $K = L^+$.*

Proof : If $U(L)/E(L)$ and $U(K)/E(K)$ are isomorphic, then their ranks coincide and Theorem 3.13 gives

$$r_1(K) + r_2(K) = r_1(L) + r_2(L).$$

Putting $n = [L : K]$ we get

$$r_1(L) + 2r_2(L) = [L : \mathbb{Q}] = n[K : \mathbb{Q}] = nr_1(K) + 2nr_2(K),$$

thus

$$r_2(L) = (n-1)r_1(K) + (2n-1)r_2(K),$$

and

$$r_1(L) = r_1(K) + r_2(K) - r_2(L) = (2-n)r_1(K) + 2(1-n)r_2(K).$$

Since $r_1(L) \geq 0$, the last equality implies $n \leq 2$, thus $n = 2$ and $r_1(L) = -2r_2(K)$, which is possible only if $r_1(L) = r_2(K) = 0$, showing that L is totally complex and K is totally real. The converse implication is obvious, and the last assertion results from the observation that $[L : K] = 2$ is a prime, and therefore there are no intermediate fields between K and L. □

A totally complex field, which is a quadratic extension of a totally real field is called a *CM-field*. The last proposition establishes a characteristic property of such fields.

Corollary 1. *If K is a proper subfield of L, then the factor group $U(L)/U(K)$ is finite if and only if L is a CM-field, and $K = L^+$.*

Proof : Observe first that the embedding $U(K) \longrightarrow U(L)$ implies that $A(K) = U(K)/E(K)$ is a subgroup of $A(L) = U(L)/E(L)$. If the group $U(L)/U(K)$ is finite, then $A(K)$ is of finite index in $A(L)$, and, since they are both free Abelian groups, their ranks coincide, whence they are isomorphic. Now the last proposition implies the first implication. To obtain the converse implication observe that if L is a CM-field and $K = L^+$, then the proposition shows that $A(K) \subset A(L)$ are free Abelian groups of the same rank, hence the index $[A(L) : A(K)]$ is finite. □

There exist fields L having a system of fundamental units lying in a proper subfield $K \subset L$, i.e., $U(L) = E(L)U(K)$. We prove now that such situation arises when $L/\mathbb{Q}$ is a complex cyclic extension.

Theorem 3.21. *If L/Q is cyclic, then L has a fundamental system of real units.*

Proof : If L is real itself, then there is nothing to prove. So assume that L is a complex cyclic extension of degree n. Then $n = 2r_2$ is even and the unit rank equals $r = n/2 - 1$. Fix a system $\epsilon_1, \ldots, \epsilon_r$ of fundamental units of L, let σ be a fixed generator of the Galois group $G(L/\mathbb{Q})$, let ζ be a generator of $E(L)$, and put $N = \#E(L)$.

Consider the matrix $A = [a_{ij}]$, whose elements are uniquely defined by

$$\sigma(\epsilon_i) = \zeta^{a_i} \prod_{j=1}^{r} \epsilon_j^{a_{ij}} \quad (i = 1, 2, \ldots, r; a_i, a_{ij} \in \mathbb{Z}).$$

We shall prove that A satisfies

$$A^r + A^{r-1} + \cdots + A + E = 0, \tag{3.5}$$

E being the unit $r \times r$ matrix.

If we put, for $k = 1, 2, \ldots, r$,

$$\sigma^k(\epsilon_i) = \zeta^{a_i(k)} \prod_{j=1}^{r} \epsilon_j^{a_{ij}(k)} \quad (i = 1, 2, \ldots, r),$$

then we get $[a_{ij}(k)] = A^k$, and this implies in turn

$$T_i = \epsilon_i \sigma(\epsilon_i) \cdots \sigma^r(\epsilon_i) = \zeta^{b_i} \prod_{j=1}^{r} \epsilon_j^{b_{ij}} \quad (i = 1, 2, \ldots, r),$$

with $[b_{ij}] = A^r + A^{r-1} + \cdots + A + E$. Thus we have to show that all b_{ij}'s vanish, or, which means the same, that all T_i's are roots of unity. Since $\sigma^{r+1} = \sigma^{n/2}$ is the only element of order two in $Gal(L/\mathbb{Q})$, it coincides with complex conjugation, and we obtain

$$\sigma^{n/2}(\epsilon_i)\sigma^{n/2+1}(\epsilon_i) \cdots \sigma^{n-1}(\epsilon_i) = \sigma^{n/2}(\epsilon_i \sigma(\epsilon_i) \cdots \sigma^r(\epsilon_i)) = \sigma^{n/2}(T_i) = \bar{T}_i,$$

which implies

$$N_{L/\mathbb{Q}}(\epsilon_i) = \epsilon_i \sigma(\epsilon_i) \cdots \sigma^{n-1}(\epsilon_i) = T_i \bar{T}_i = |T_i|^2.$$

Proposition 3.10 leads now to $|T_i| = 1$ for $i = 1, 2, \ldots, r$. We shall now show that $|\sigma^k(T_i)| = 1$ holds for $k = 1, 2, \ldots, n-1$. In fact, for $k = 1$ we have

$$\sigma(T_i) = \sigma(\epsilon_i) \cdots \sigma^{1+r}(\epsilon_i) = T_i \epsilon_i^{-1} \bar{\epsilon}_i,$$

whence $|\sigma(T_i)| = 1$, and if $|\sigma^{k-1}(T_i)| = 1$ holds, then the equalities

$$\begin{aligned} \sigma^k(T_i) &= \sigma^{k-1}(\sigma(T_i)) = \sigma^{k-1}(T_i \epsilon_i^{-1} \bar{\epsilon}_i) \\ &= \sigma^{k-1}(T_i)\sigma^{k-1}(\epsilon_i^{-1})\overline{\sigma^{k-1}(\epsilon_i)} \\ &= \sigma^{k-1}(T_i)\overline{\sigma^{k-1}(\epsilon_i)}/\sigma^{k-1}(\epsilon_i) \end{aligned}$$

show that $|\sigma^k(T_i)| = 1$. Theorem 2.5 (i) enables us to conclude that all T_i's are roots of unity, and so A satisfies (3.5). This implies in particular that $A^{n/2} = E$, hence for $i = 1, 2, \ldots, r$ the equalities

$$\sigma^{n/2}(\epsilon_i) = \zeta^{t_i} \epsilon_i$$

hold with

$$t_i = \sum_{j=1}^{r} a_j(\delta_{ij}\beta^r + a_{ij}\beta^{r-1} + a_{ij}(2)\beta^{r-2} + \cdots + a_{ij}(r)), \tag{3.6}$$

where β is defined by $\sigma(\zeta) = \zeta^\beta$ and $0 \leq \beta < N$, and δ_{ij} is the Kronecker symbol.

By Proposition 3.11 N is even, therefore in view of

$$\zeta^{-1} = \bar{\zeta} = \sigma^{n/2}(\zeta) = \zeta^{\beta^{n/2}}, \quad \beta^{n/2} + 1 \equiv 0 \pmod{N},$$

we conclude that β is odd.

Applying once more (3.5) and using the oddness of β we see that the terms in parentheses in (3.6) are all even, thus the same holds for the t_i's. Putting $t_i = 2u_i$ and $\eta_i = \zeta^{u_i}\epsilon_i$ for $i = 1, 2, \ldots, r$ we obtain that the η_i's form a system of fundamental units. Moreover, due to $\bar{\eta}_i = \sigma^{n/2}(\eta_i) = \zeta^{-u_i} s^{n/2}(\epsilon_i) = \zeta^{-u_i} \cdot \zeta^{t_i}\epsilon_i = \zeta^{u_i}\epsilon_i = \eta_i$, they are all real. □

Corollary. *If p is an odd prime and $n \geq 1$, then every unit ϵ of the cyclotomic field $L = \mathbb{Q}(\zeta_{p^n})$ can be written in the form $\epsilon = \zeta \cdot \eta$, where $\zeta \in E(L)$ and $\eta \in U(L^+)$.*

Proof : It suffices to note that the extension $L/\mathbb{Q}$ is cyclic and to apply the preceding theorem. □

A similar, but weaker, conclusion is true for a large class of normal CM-fields:

Theorem 3.22. *If K is CM-field such that the extensions $K/\mathbb{Q}$ and $K^+/\mathbb{Q}$ are both normal, then every unit ϵ of K can be written in the form $\epsilon = \zeta\eta$, where ζ is a root of unity, whose square lies in K and η is a real unit, whose square lies in K^+.*

Proof : We need a lemma:

Lemma 3.23. *Under the assumptions of the theorem the complex conjugation acts trivially on $U(K)/E(K)$, i.e., for every unit ϵ of K we have $\bar{\epsilon} = u\epsilon$, with $u \in E(K)$.*

Proof : Observe first that the normality of $K^+/\mathbb{Q}$ implies that the complex conjugation s lies in the center of $G = Gal(K/\mathbb{Q})$. Indeed, the group $\{e, s\}$ corresponds to K^+ by Galois theory, hence it is a normal subgroup of G. Thus for g in G we must have either $gsg^{-1} = e$, or $gsg^{-1} = s$. However, the first equality gives $s = e$, a contradiction, thus we must have $sg = gs$. If $\epsilon \in U(K)$, then for $u = \bar{\epsilon}\epsilon^{-1}$ we have $|u| = 1$, whence for all g in G we get

$$1 = g(u\bar{u}) = g(u)g(\bar{u}) = g(u)\overline{g(u)},$$

thus $|g(u)| = 1$ and $\overline{|u|} = 1$ follows. By Theorem 2.5 (i) u must be a root of unity, and the lemma follows. □

If now ϵ lies in $U(K)$, then by the lemma we have $\bar{\epsilon} = u\epsilon$, with a suitable root of unity $u \in K$. The number $|\epsilon|$ is a real unit, being a root of $X^2 - \epsilon\bar{\epsilon}$. If we put $\zeta = \epsilon/|\epsilon|$, then $\zeta^2 = \epsilon^2/|\epsilon|^2 = \epsilon\bar{\epsilon}^{-1} = u^{-1}$, hence ζ is a root of unity. Since $\epsilon\bar{\epsilon}$ lies in K^+ our assertion follows with $\eta = |\epsilon|$. □

5. Certain subgroups of the group $U(K)$ of units are also of importance. Let I be a non-zero ideal of R_K, and denote by $U(K,I)$ the subgroup of $U(K)$, consisting of all units of K, congruent to unity mod I. Similarly, let $U^+(K,I)$ be the group of all totally positive units of K, congruent to unity mod I. In the case $I = R_K$ we shall simply write $U^+(K)$ for this group. It consists of all totally positive units of K.

The structure of these groups is described by the following result:

Proposition 3.24. *If $r(K) \geq 1$, then the group $U^+(K,I)$ is the product of the cyclic group consisting of all totally positive roots of unity contained in K, which are congruent to* 1 mod I *and r copies of the cyclic infinite group. The group $U(K,I)$ is the product of the cyclic group consisting of all roots of unity of K, congruent to* 1 mod I *and r copies of the cyclic infinite group.*

Proof : Since the $2\Phi(I)$th power of every element of $U(K)$ lies in $U^+(K,I)$ and $U(K)/E(K)$ is the rth power of the cyclic infinite group, the same holds for $U^+(K,I)/(E(K) \cap U^+(K,I))$, and our assertion about $U^+(K,I)$ follows. The same argument applies to $U(K,I)$. □

This proposition shows that for a given ideal I one can find units $\eta_1, \ldots, \eta_r$ in $U^+(K,I)$ and in $U(K,I)$ such that every element of these groups can be uniquely written in the form $\zeta \eta_1^{n_1} \cdots \eta_r^{n_r}$ with rational integral exponents n_i, ζ being a root of unity lying in $U^+(K,I)$ and $U(K,I)$, respectively. The units $\eta_1, \ldots, \eta_r$ are called the *fundamental totally positive units* mod I *of* K, and the *fundamental units* mod I *of* K, respectively.

The regulators of a system of fundamental units mod I and of a system of fundamental totally positive units mod I are denoted by $R_I(K)$ and $R_I^+(K)$, respectively.

Now we shall establish the connection between the class numbers $h(K)$, $h^*(K)$, $h_I(K)$ and $h_I^*(K)$. To do this we have to introduce some notation. Consider the map $f : K^* \longrightarrow D(K)$, as defined in subsection 1 of Sect.2 and look at the images of $U(K)$ and $U(K,I)$ under this mapping. They obviously lie in the 2-group generated by the infinite prime divisors, thus they are finite, and we may write, say, $\#f(U(K)) = 2^s$ and $\#f(U(K,I)) = 2^t$. For our immediate purpose it is important to observe that $\#f(U(K))$ equals the number of possible signatures of units, and $\#f(U(K,I))$ equals the number of possible signatures of units congruent to unity mod I. Moreover, denote by $\psi(I)$ the number of residue classes mod I which can be represented by units of K.

Theorem 3.25. *Let I be a non-zero ideal of R_K. Then we have:*

(i) $H(K) \sim H_I(K)/P_I^{(0)}(K)$, $h_I(K) = h(K)\Phi(I)/\psi(I)$,

(ii) $H_I(K) \sim H_I^*(K)/P_I^*(K)$, $h_I^*(K) = 2^{r_1 - t} h_I(K)$,

(iii) $H(K) \sim H^*(K)/P_{R_K}^*(K)$, $h^*(K) = 2^{r_1 - s} h(K)$, *where $P_I^*(K)$ denotes the group of classes of $H_I^*(K)$ consisting of principal ideals having*

a generator congruent to unity mod I, *and* $P_I^{(0)}$ *denotes the subgroup of* $H_I(K)$ *consisting of classes containing principal ideals.*

Proof : If two ideals are in the same class in $H_I(K)$, then they are also in the same class in $H(K)$. This simple remark shows the existence of a canonical homomorphism of $H_I(K)$ in $H(K)$, carrying every class of $H_I(K)$ in the class of $H(K)$ containing each of its ideals. Corollary 6 to Proposition 1.14 shows that every class in $H(K)$ contains an ideal relatively prime to I, and so the homomorphism just defined is in fact surjective. Its kernel being obviously $P_I^{(0)}$, we arrive at the first assertion of (i). To prove the second assertion we have to evaluate $P_I^{(0)}$. It consists of a union of $h_I(K)/h(K)$ classes of $H_I(K)$ and this is the number we have to find. Let E be the unit class of $H(K)$ and let $A \in E$ satisfy $(A, I) = 1$. If a is any generator of A, then other generators have the form ϵa with $\epsilon \in U(K)$. Therefore with every such A we may associate a set $\Lambda_A = \{\lambda_1, \ldots, \lambda_k\}$ (with $k = \psi(I)$) of residue classes mod I, namely of those, which have a representative generating the ideal A. Obviously, two ideals $A, B \in E$, satisfying $(AB, I) = 1$ are in the same class of $H_I(K)$ if and only if the sets Λ_A and Λ_B coincide. Since there are $\Phi(I)/\psi(I)$ such sets, we arrive at $h_I(K)/h(K) = \Phi(I)/\psi(I)$, proving (i).

The proof of (ii) follows the same pattern. We consider the canonical surjective homomorphism $H_I^*(K) \longrightarrow H_I(K)$ with kernel $P_I^*(K)$. Consider the principal class of $H_I(K)$, which consists of all principal ideals of the form aR_K with $a \equiv 1 \,(\mathrm{mod}\ I)$. We have to find the number of classes of $H_I^*(K)$ formed by such ideals. If $a \equiv 1 \,(\mathrm{mod}\ I)$ and a generates an ideal A, then every other generator of A congruent to unity mod I must be equal to ϵa for some $\epsilon \in U(K, I)$. Associate with every such ideal a set $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ (with $m = 2^t$) of signatures of its generators congruent to unity mod I. Obviously, two ideals from the principal class of $H_I^*(K)$ are in the same class of $H_I(K)$ if and only if their systems of signatures coincide. By Proposition 2.2 (i) every possible signature can be represented by an integer congruent to unity mod$I$, whence there are exactly $2^{r_1 - t}$ systems Γ, proving (ii).

Finally, (iii) is a special case of (ii), with $I = R_K$. □

Corollary 1. *The equality* $H(K) = H^*(K)$ *holds if and only if* K *contains units of every signature. This holds, in particular, for all totally complex fields.* □

Corollary 2. *If* K *is a real quadratic field and* ϵ *is its fundamental unit, then*

$$h^*(K) = \begin{cases} 2h(K) & \text{if } N_{K/\mathbb{Q}}(\epsilon) = 1, \\ h(K) & \text{otherwise.} \end{cases}$$

Proof : In this case the factor $2^{r_1 - s}$ equals either 1 or 2, the first possibility arising when there are units of every signature. One sees directly that this

happens if and only if there is a unit of negative norm, but this implies that the norm of the fundamental unit is negative. □

Corollary 3. *If K is totally real, then $H(K) = H^*(K)$ holds if and only if every totally positive unit of K is a square in K.*

Proof : Let $U^2(K)$ be the group of all squares of units of K. Theorem 3.13 and Proposition 3.11 imply that the quotient $U(K)/U^2(K)$ is isomorphic to C_2^n with $n = [K : \mathbb{Q}]$, and since the number of possible signatures equals 2^n and $U^2(K) \subset U^+(K)$, it follows that the ratio

$$\#\left(U^+(K)/U^2(K)\right) = \#(U(K)/U^2(K))/\#(U(K)/U^+(K))$$

equals 1 if and only if $\#U(K)/U^+(K) = 2^n$. However the index of $U^+(K)$ in $U(K)$ equals the number of unit signatures in K, and it remains to apply Corollary 1. □

To state the next corollary, denote by $e_q(A)$ the number of the invariants of the finite Abelian group A which are divisible by a prime power q, i.e., the number of cyclic factors of order divisible by q in a decomposition of A into cyclic summands. Note that $e_q(A)$ does not depend on the decomposition.

Corollary 4. *For $n \geq 1$ we have*

$$e_{2^n}(H(K)) = e_{2^n}(H^*(K)) + A(n) - A(n-1),$$

where $2^{A(n)}$ is the number of classes in $P^*_{R_K}(K)$ which are 2^n-th powers of elements of $H^*(K)$.

Proof : Write, for brevity, H, H^* and P for $H(K)$, $H^*(K)$ and $P^*_{R_K}(K)$. For every Abelian finite group A and $n \geq 1$ w have

$$e_{2^n}(A) = \dim_{\mathbb{F}_2} A^{2^{n-1}}/A^{2^n},$$

since every group C_2^N can be regarded as a linear space over $\mathbb{F}_2$ and $A^{2^{n-1}}/A^{2^n}$ is of this form.

The natural map $H^* \longrightarrow H$ induces the exact sequence

$$0 \longrightarrow X \longrightarrow (H^*)^{2^{n-1}}/(H^*)^{2^n} \longrightarrow H^{2^{n-1}}/H^{2^n} \longrightarrow 0,$$

(where $X = (P \cap (H^*)^{2^{n-1}})/(P \cap (H^*)^{2^n})$ of linear spaces. Hence

$$\begin{aligned} e_{2^n}(H^*) &= e_{2^n}(H) + \dim_{\mathbb{F}_2} X \\ &= e_{2^n}(H) + \log_2(\#X) = e_{2^n}(H) + A(n-1) - A(n), \end{aligned}$$

giving our assertion. □

Corollary 5. *The 2-ranks of the groups $H(K)$ and $H^*(K)$ coincide if and only if every class of $H^*(K)$ consisting of principal ideals is a square.*

Proof : This follows from the case $n = 1$ of the preceding corollary. □

6. In the case of a normal extension $K/\mathbb{Q}$ one may ask about the existence of a system of fundamental units which are all conjugate, or at least of a system of $r(K)$ conjugate independent units, where independence means the linear independence of their images in the real n-space under the mapping considered in the proof od Dirichlet's theorem. The main result of this type is due to Minkowski:

Theorem 3.26. *If the extension $K/\mathbb{Q}$ is normal, then there exists a system of $r(K)$ independent conjugated units.*

Proof : Let $[K : \mathbb{Q}] = n$, and denote by G the Galois group of K. Assume first that the extension $K/\mathbb{Q}$ is totally complex, and let $\tau \in G$ be the complex conjugation. Writing $G = \{g_i, \tau g_i : \ i = 1, 2, \ldots, s = n/2\}$ we obtain that every normalized Archimedean valuation of K is of the form $v_i(x) = |g_i(x)|^2$ $(i = 1, 2, \ldots, s)$. As in the proof of Theorem 3.12 we obtain the existence of a unit ϵ with $v_1(\epsilon) > 1$ and $v_i(\epsilon) < 1$ for $i \neq 1$. Now consider the units $\epsilon, g_2^{-1}(\epsilon), \ldots, g_s^{-1}(\epsilon)$. We have

$$v_j(g_k^{-1}(\epsilon)) = |g_j g_k^{-1}(\epsilon)|^2 \begin{cases} > 1 & \text{if } j = k, \\ < 1 & \text{otherwise.} \end{cases}$$

Therefore, if we put $\eta = \epsilon\tau(\epsilon)$, then the reasoning used in the proof of Theorem 3.12 shows that if remove one element from the set $\{g_i(\eta) : \ i = 1, 2, \ldots, s\}$, then the remaining elements form an independent set of conjugate elements.

The same type of argument applies to the case when K is totally real. In this case we have $G = \{g_i : \ i = 1, 2, \ldots, n\}$, every Archimedean valuation has the form $v_i(x) = |g_i(x)|$, and $n - 1$ conjugates of ϵ, obtained as above, form an independent set of units. □

The last theorem gives some information about the action of the Galois group on the group of units. To be more precise, let $\mathbb{Z}[G]$ be the group-ring of a given finite group G over $\mathbb{Z}$, i.e., the free Abelian group generated by elements of G, in which one defines multiplication by means of

$$\sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{t \in G} \Big(\sum_{gh = t} a_g b_h \Big) t.$$

If $K/\mathbb{Q}$ is normal with Galois group G, then every subgroup D of the multiplicative group K^*, which is G-invariant, acquires the structure of a $\mathbb{Z}[G]$-module, where an element $A = \sum_{g \in G} a_g g$ of $\mathbb{Z}[G]$ acts on $x \in D$ by

$$Ax = \prod_{g \in G} g(x)^{a_g}.$$

We shall be interested in the case $D = U(K)$. Since $E(K)$ is G-invariant, the factor group $U_0(K) = U(K)/E(K)$ is also a $\mathbb{Z}[G]$-module. Observe now that if $a \in U(K)$ is such that $r(K)$ of its conjugates satisfy Theorem 3.26, then the submodule $U_1(K)$ of $U_0(K)$ generated by the image of a is of finite index. Indeed, both $U_1(K)$ and $U_0(K)$ are free Abelian groups of the same rank. We may thus state Theorem 3.26 in the following form:

Theorem 3.26a. *If $K/\mathbb{Q}$ is normal with Galois group G, then the $\mathbb{Z}[G]$-module $U(K)/E(K)$ contains a cyclic submodule of finite index.* □

We may ask under what circumstances will $U(K)/E(K)$ be itself cyclic. If this happens, then every unit representing the generator of $U(K)$ is called a *Minkowski unit*. Moreover, if there exists a unit u whose certain conjugates form a system of fundamental units, then u is called a *strong Minkowski unit*.

Proposition 3.27. *A strong Minkowski unit is a Minkowski unit, and if K is real, then these notions coincide.*

Proof : If $\epsilon_1, \ldots, \epsilon_r$ is a system of conjugated fundamental units, then the image of ϵ_1 in $U_0(K)$ generates $U_0(K)$, whence ϵ_1 is a Minkowski unit.

If K is real and ϵ is a Minkowski unit, then every unit u of K can be written in the form

$$u = \pm \prod_{g \in G} g(\epsilon)^{a_g}$$

with $a_g \in \mathbb{Z}$. Since

$$\prod_{g \in G} g(\epsilon) = N_{K/\mathbb{Q}}(\epsilon) = \pm 1,$$

we get, with $e = id_K$ being the unit of G,

$$\epsilon = \pm \prod_{g \neq e} g(\epsilon)^{-1},$$

whence

$$u = \pm \prod_{g \neq e} g(\epsilon)^{a_g - a_e},$$

i.e., the set $\{g(\epsilon) : g \neq e\}$ is a set of generators of $U(K)$, and since it contains $[K : \mathbb{Q}] - 1 = r(K)$ elements, it is a set of fundamental units. □

The problem in which fields there exist Minkowski units or strong Minkowski units is unsolved, except in certain special cases. We present now one of them.

Theorem 3.28. *If p is an odd prime such that the cyclotomic field $\mathbb{Q}(\zeta_p)$ has class-number 1, and $K/\mathbb{Q}$ is a cyclic extension of degree p, then K has a strong Minkowski unit.*

Proof : We start with an easy lemma:

Lemma 3.29. *If $K/\mathbb{Q}$ is normal with Galois group G and*

$$N = \sum_{g \in G} g \in \mathbb{Z}[G],$$

then the principal ideal of $\mathbb{Z}[G]$, generated by N equals $N\mathbb{Z}$. If Λ denotes the factor ring $\mathbb{Z}[G]/N\mathbb{Z}$, then $U_0(K) = U(K)/E(K)$ becomes a Λ-module in a canonical way.

Proof : The ideal generated by N obviously equals $N\mathbb{Z}[G]$ and contains $N\mathbb{Z}$. If now $b = \sum_{b \in G} b_g g \in \mathbb{Z}[G]$ and $a = Nb \in N\mathbb{Z}[G]$, then $a = \left(\sum_{g \in G} b_g\right) N \in N\mathbb{Z}$, and $N\mathbb{Z}[G] = N\mathbb{Z}$ follows. The second assertion results from the observation that for $u \in U(K)$ we have

$$Nu = \prod_{g \in G} g(u) = N_{K/\mathbb{Q}}(u) = \pm 1 \in E(K),$$

and we see that N acts trivially on $U_0(K)$. Therefore the action of $\mathbb{Z}[G]$ on $U_0(K)$ induces canonically the action of Λ. □

The theorem follows now without much effort. Indeed, in our case the group G is cyclic, so let g be its generator. Put also $R = \mathbb{Z}[\zeta_p]$. The homomorphism $\varphi : \mathbb{Z}[G] \longrightarrow R$ of rings, defined by $\varphi(g) = \zeta_p$ is surjective and its kernel equals $N\mathbb{Z}$, with $N = e + g + g^2 + \cdots + g^{p-1}$. Indeed, $N\mathbb{Z}$ lies in the kernel because of $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$, and if $a = \sum_{j=0}^{p-1} a_j g^j$ lies in the kernel, then

$$0 = \varphi(a) = \sum_{j=0}^{p-1} a_j \zeta_p^j = \sum_{j=0}^{p-2} (a_j - a_{p-1}) \zeta_p^j,$$

thus by Theorem 2.20 we get $a_0 = a_1 = \ldots = a_{p-1}$, i.e., $a \in N\mathbb{Z}$. It follows that R and $\mathbb{Z}[G]/N\mathbb{Z}$ are isomorphic rings, and the lemma shows that $U_0(K)$ is a finitely generated R-module. Since by Theorem 2.20 R is the ring of integers of $\mathbb{Q}(\zeta_p)$, it is Dedekind, and by assumption it has class-number 1, and Theorem 1.45 implies that it is a principal ideal domain. Theorem 1.32 shows that with a suitable $m \geq 0$ the R-module $U_0(K)$ is isomorphic to $R^m \oplus T$, where T is a torsion R-module. By Proposition 1.40 T is finite, and were it non-zero, then $U_0(K)$ would contain a finite non-zero subgroup, which is absurd. By Theorem 3.13 the $\mathbb{Z}$-rank of $U_0(K)$ equals $p-1$, and since the $\mathbb{Z}$-rank of R^m is $m(p-1)$, we obtain $m = 1$. Thus $U_0(K)$ is isomorphic to R as

an R-module, and *a fortiori* as a $\mathbb{Z}[G]$-module. But R is a cyclic $\mathbb{Z}[G]$-module and thus K has a Minkowski unit. Since K is real, this unit is also a strong Minkowski unit by Proposition 3.27. □

Unfortunately, it has been shown by Uchida [71,III] that the assumptions of this theorem are satisfied only for primes $p \leq 19$.

3.4. Euclidean Algorithm

1. We shall now be concerned with fields whose rings of integers are Euclidean. It is well known that every such ring is a unique factorization domain, and so such fields have trivial class-groups. We recall the definition:

A domain R is said to be a *Euclidean domain* if there exists a function p, defined on R whose values are non-negative rational integers, satisfying the conditions

(i) One has $p(x) = 0$ if and only if $x = 0$,

and

(ii) If $a, b \in R$, $b \neq 0$, then there exist $c, r \in R$ such that $a = bc + r$ and $p(r) < p(b)$.

In earlier treatments of this subject usually the additional condition $p(ab) \geq p(b)$ for non-zero a, b was made, however it has been shown by Veldkamp [60] (see also Samuel [71]) that it is redundant, since it does not change the class of rings considered.

We shall say that an algebraic number field K is *norm-Euclidean* if the ring R_K is Euclidean with $p(x) = |N_{K/\mathbb{Q}}(x)|$. The following proposition is helpful in establishing the norm-euclidicity of a given field:

Proposition 3.30. *A field K is norm-Euclidean if and only if for every $a \in K$ there exists $t \in R_K$ with $|N_{K/\mathbb{Q}}(a - t)| < 1$.*

Proof : In our case the Euclidean condition takes the form $|N_{K/\mathbb{Q}}(a - bc)| < |N_{K/\mathbb{Q}}(b)|$, for given $a, b \neq 0$ and suitable c, all of them integers of K, and in view of the multiplicativity of the norm we may write it as

$$|N_{K/\mathbb{Q}}(ab^{-1} - c)| < 1.$$

It remains to observe that every element of K may be written as a ratio of two elements of R_K, □

Corollary. *An imaginary quadratic field K is norm-Euclidean if and only if $d(K) \in \{-3, -4, -7, -8, -11\}$.*

Proof : First we show that all listed fields are indeed norm-Euclidean. If $d(K) \in \{-4, -8\}$, then every integer of K has the form $x + y\sqrt{D}$ with $D =$

$d(K)/4$ and $x, y \in \mathbb{Z}$. If now $a + b\sqrt{D}$ $(a, b \in \mathbb{Q})$ is an arbitrary element of K and we choose $x, y \in \mathbb{Z}$ with $|a - x| \leq 1/2$ and $|b - y| \leq 1/2$, then

$$|N_{K/\mathbb{Q}}((a + b\sqrt{D}) - (x + y\sqrt{D}))| = (a - x)^2 + (b - y)^2|D| \leq \frac{1 + |D|}{4} < 1,$$

since $D \in \{-1, -2\}$.

If $d = d(K) \in \{-3, -7, -11\}$, then the integers of K have the form $(x + y\sqrt{d})/2$ with $x, y \in \mathbb{Z}$ of the same parity. If $a + b\sqrt{d} \in K$ $(a, b \in \mathbb{Q})$, then choosing first $y \in \mathbb{Z}$ so that $|b - y/2| \leq 1/4$ and afterwards $x \in \mathbb{Z}$ with $|a - x/2| \leq 1/2$ and $x \equiv y \pmod 2$, we obtain

$$\begin{aligned} |N_{K/\mathbb{Q}}((a + b\sqrt{d}) - (x/2 + (y/2)\sqrt{d}))| &= (a - x/2)^2 + (b - y/2)^2|d| \\ &\leq \frac{4 + |d|}{16} < 1. \end{aligned}$$

Now assume that K is a norm-Euclidean imaginary quadratic field and put $d = d(K)$. Consider first the case $4|d$. Put $D = d/4$ and let $a = \sqrt{D}/2$. Since K is norm-Euclidean, there exists $x + y\sqrt{D} \in R_K$ $(x, y \in \mathbb{Z})$ with

$$|N_{K/\mathbb{Q}}(x + (y - 1/2)\sqrt{D})| < 1,$$

i.e.,

$$x^2 + (y - 1/2)^2|D| < 1.$$

However for every $y \in \mathbb{Z}$ one has $(y - 1/2)^2 \geq 1/4$, whence $|D|/4 < 1$, leading to $d \in \{-4, -8\}$.

If $4 \nmid d$, then consider $a = (1 + \sqrt{d})/4$. For certain $x, y \in \mathbb{Z}$ we have $|N_{K/\mathbb{Q}}(a - (x + y\sqrt{d})/2)| < 1$, thus

$$\left(\frac{1}{4} - \frac{x}{2}\right)^2 + \left(\frac{1}{4} - \frac{y}{2}\right)^2 |d| < 1.$$

However for all $m \in \mathbb{Z}$ one has $|1/4 - m/2| \geq 1/4$, whence $1 + |d| < 16$, leaving us with $d \in \{-3, -7, -11\}$. □

2. The determination of all real quadratic norm-Euclidean fields is much more difficult. Heilbronn [38a] proved that their number is finite, and later, through efforts of several authors, it was established that their discriminants are equal to 5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73 and 76, The final step was done by Chatland and Davenport [50]. We shall not present the proof of this result, belonging rather to the geometry of numbers, and prove only the following theorem:

Theorem 3.31. *The real quadratic fields with discriminants* $d = 5$, 8, 12, 13, 17, 21, 24, 28 *and* 29 *are norm-Euclidean.*

Proof : We need a simple lemma:

Lemma 3.32. *If $0 \leq a < 2$ and $a \neq 5/4$, then to every real x there corresponds a real y satisfying $x - y \in \mathbb{Z}$ and $|y^2 - a| < 1$.*

Proof : If $a = 0$, then a suitable number from the interval $(-1/2, 1/2]$ will do. The assertion will hold also with a suitable number y satisfying $1/2 \leq |y| \leq 1$, if $0 < a < 5/4$, and with some y with $1 \leq |y| \leq 3/2]$, if $5/4 < a < 2$. □

Consider now $d = 8, 12, 24$ and 28. Then the integers of $Q(\sqrt{d})$ are of the form $x + y\sqrt{D}$ with $D = d/4$ and $x, y \in \mathbb{Z}$. By Proposition 3.30 it suffices to find for every pair a, b of rationals a pair x, y of rational integers satisfying

$$|(a - x)^2 - D(b - y)^2| < 1.$$

Choose $y \in \mathbb{Z}$ with $|b - y| \leq 1/2$. Then

$$D(b - y)^2 \leq D/4 \leq 7/4 \quad \text{and} \quad D(b - y)^2 \neq 5/4,$$

since $D \neq 5$. We may thus use Lemma 3.32 to obtain the required inequality.

The remaining fields have integers of the form $x + y\omega$ with $\omega = (1 + \sqrt{d})/2$ $(x, y \in \mathbb{Z})$, and so we have to show that for every pair of rational a, b we may find $x, y \in \mathbb{Z}$ with $|(a - x - y/2)^2 - d(b - y/2)^2| < 1$.

Choose $y \in \mathbb{Z}$ with $|2b - y| \leq 1/2$. Then $d(b - y/2)^2 \leq d/16 \leq 29/16$ and since $d(b - y/2)^2 \neq 5/4$, because in case $d = 5$ we have $d(b - y/2)^2 \leq 5/16$, we may apply Lemma 3.32 as in the preceding case, □

The natural question, whether a Euclidean algebraic number field must necessarily be norm-Euclidean has a positive answer in the case of imaginary quadratic fields, but in general this fails to be true. Clark [94] proved that $\mathbb{Q}(\sqrt{69})$ is Euclidean, but not norm-Euclidean (cf. Niklasch [94]), and in Clark [96] he produced two examples of such cubic fields.

Proposition 3.33. *If K is an Euclidean imaginary quadratic field, then it is norm-Euclidean, hence is one of the fields listed in the Corollary to Proposition 3.30.*

Proof : Assume that $|d(K)| > 11$ and let p be an Euclidean norm in R_K. Choose $t \in R_K$ different from $0, \pm 1$ so that

$$p(t) = \min\{p(x) : \ x \in R_K, x \neq 0, \pm 1\}.$$

Then for every $b \in R_K$ we can find $q \in R_K$ with $b - qt \in \{0, \pm 1\}$, whence we get $N_{K/\mathbb{Q}}(t) \leq 3$ by the Corollary to Proposition 2.13.

Put

$$D = \begin{cases} d(K)/4 & \text{if } 4 | d(K), \\ d(K) & \text{otherwise,} \end{cases}$$

and observe that if $D \not\equiv 1 \pmod 4$, then $t = x + y\sqrt{D}$ with $x, y \in \mathbb{Z}$, and because $|d(K)| > 11$ implies $|D| \geq 3$, hence $x^2 + |D|y^2 \leq 3$ can happen only if $D = -3 \equiv 1 \pmod 4$, contradiction.

Similarly, if $D \equiv 1 \pmod 4$, then $t = (x + y\sqrt{D})/2$ with $x, y \in \mathbb{Z}$ of the same parity. If x and y are both even, then the preceding argument leads to a contradiction. If x, y are both odd, then

$$12 \geq N_{K/\mathbb{Q}}(x + y\sqrt{D}) = x^2 + y^2|D| \geq 1 + |D|,$$

and so $|d| = |D| \leq 11$, again giving a contradiction. □

In Chap. 4 we shall prove that the field $Q(\sqrt{-19})$ has class-number 1, and so its ring of integers is an example of a Dedekind unique factorization domain which is not Euclidean.

To conclude this chapter we prove a result which in the case of rings of integers goes back to Dedekind [31], and was obtained in its most general form by Hasse [28]. It gives a sufficient condition for a domain to be a principal ideal domain. In the case of Dedekind domains this condition is also necessary, and hence leads to another characterization of fields with trivial class group. We have included this result in the section dealing with Euclidean rings, since there is a formal resemblance between the conditions of the theorem and the definition of euclidicity.

Theorem 3.34. *(i) Let R be an integral domain and assume that there is a function f defined in R with values in the set of nonnegative integers such that*

(a) $f(x) = 0$ holds if and only if $x = 0$,

(b) If $0 < f(y) \leq f(x)$ and $y \nmid x$, then for suitable $a, b \in R$ one has

$$0 < f(ax - by) < f(y).$$

Then R is a principal ideal domain.

(ii) If R is a Dedekind domain with trivial class group, then there exists a function f, satisfying $f(xy) = f(x)f(y)$ and the conditions (a) nd (b).

Proof : (i) Assume that f satisfies (a) and (b), and let I be a non-zero ideal of R. Choose $y \in I$ with minimal positive value of f, and let $x \in I$ be non-zero. Then $0 < f(y) \leq f(x)$, and if y would not divide x, then by (b) there would exist $a, b \in R$ with $0 < f(ax - by) < f(y)$, contrary to the choice of y, since $ax - by$ lies in I. Hence $x = ry$ with some $r \in R$, and we see that I is principal, generated by y.

(ii) If R is a Dedekind domain with trivial class-group, then put $f(0) = 0$, $f(u) = 1$ for all invertible elements $u \in R$ and $f(\pi) = 2$ for elements π generating prime ideals. Extending f to all R by multiplicativity we get a function satisfying the conditions (a) and (b) in part (i). □

Corollary. *An algebraic number field K has a trivial class group if and only if the function $f(x) = |N_{K/Q}(x)|$ satisfies the condition (b).*

Proof : The sufficiency follows immediately from the theorem, since f obviously satisfies the conditions (a) and (b), To prove its necessity put $f(x) = |N_{K/Q}(x)|$ and assume that $x, y \in R_K$ satisfy $0 < f(y) \leq f(x)$ and $y \nmid x$. The ideal $xR_K + yR_K$ is principal, equal to zR_K, say. Then $y = rz$ with some $r \in R_K$ which is not invertible, because otherwise we would have $y|z$ which in view of $z|x$ would give $y|x$, contrary to our assumption. Therefore $f(z) < f(y)$. Moreover with suitable $a, b \in R_K$ we have $ax - by = z$ and so we get

$$0 < f(ax - by) = f(z) < f(y),$$

as asserted. □

3.5. Notes to Chapter 3

1. It has been assumed for a long time that the theory of ideals in rings of integers owes its existence to the unsuccessful attempts of Kummer to prove Fermat's Last Theorem in its full generality. Later research however has shed some doubt on this story, and now it seems more likely that Kummer's work on ideal numbers, which led later Dedekind to introduce ideals, has been motivated by his research concerning reciprocity laws for power residues. See Edwards [77] and Neumann [81a] on this topic.

Ideal numbers, whose purpose was to restore unique factorization in rings of algebraic integers were introduced by Kummer [47a,b] in case of integers of $\mathbb{Q}(\zeta_p)$ with prime p. He did the same for arbitrary cyclotomic fields in [56] and for fields $\mathbb{Q}(\zeta_p, \sqrt[p]{a})$, called now Kummerian, in [59]. For subfields of cyclotomic fields this theory was developed in Fuchs [63], [66]. Kummer's ideal numbers lay outside the considered field K, but, adjoined to it, provided a set of numbers closed under multiplication and having the unique factorization property. In modern language these numbers correspond roughly to the ideals of R_K. In the set of ideal numbers Kummer introduced the notion of equivalence, and was led in this way to the class-number of cyclotomic fields.

Modern treatment of ideal numbers was introduced by Hecke [18], and is still used in certain parts of the analytic theory of algebraic numbers. See Albu, Nicolae [95] for the proof of Hecke's assertion that the adjoining of all ideal numbers to a field K leads to its extension of degree $h(K)$.

Ideal theory in rings of integers was created by Dedekind [71]. His method was applicable in a uniform way to all algebraic number fields, and this was its advantage over Kummer's approach. Other proofs of Dedekind's fundamental result, the unique factorization theorem for ideals, were later supplied by Kronecker [82] and Hilbert [94b].

Kronecker [82] founded his theory of algebraic numbers on the theory of forms. Its outline may be found in Hilbert [97] and H.Weber [96b]. Kronecker's theory had a much better reception than that of Dedekind, although Kronecker's paper was rather difficult to decipher, whereas Dedekind wrote very clearly. Modern expositions of Kronecker's theory were given in Del Corso [95], Edwards [90], Flanders [60], Weyl [40]. For Dedekind's comments on Kronecker's approach see Edwards, Neumann, Purkert [82] (cf. Edwards [80],[83]). Kronecker's theory can be translated into the language of ideals by associating with every form F the ideal generated by its coefficients, the *content* of F. An axiomatic characterization of the content of a form was given in Krakowski [65]. Cf. Dedekind [92], Hurwitz [94], [95a], Mertens [94].

Some ideas of Kronecker were developed by Hensel, who introduced p-adic numbers and used them for studying algebraic number fields. See Chap. 5 for more details.

Another approach was adopted by Zolotarev [80]. It is based on the notion of p-integral numbers, and is closely related to Hensel's p-adic method. For its exposition see Chebotarev [30], [37a], [47].

A method based on a kind of ideal numbers determined by infinite systems of linear congruences, every finite subsystem of which is solvable was introduced by Prüfer [25] (see also von Neumann [26]).

The method of Krull [51] was based on the consideration of homomorphisms of the multiplicative group of a field into free Abelian groups. A fresh exposition may be found in Borevich, Shafarevich [64]. See also Frey, Geyer [72], Koch [66], Skula [70].

The theory of infinite algebraic extensions of $\mathbb{Q}$ was initiated by Stiemke [26] and Krull [28b,d], and developed in Gut [37], Herbrand [31c], [32b], Moriya [34], Scholz [43].

2. Theorem 3.1 is due to Kűrschak [13], and Theorem 3.3 to Ostrowski (the Archimedean case in [18] and the non-Archimedean case in [35]). Cf. Artin [32b], Mac Lane [36]. For a constructivistic approach see Mines, Richman [81], [84]. The importance of the product formula (Theorem 3.5) was stressed by Artin and Whaples [45], [46], who used it for an axiomatical characterization of algebraic number fields, and also for developing anew the fundamental results of this their theory, including Dirichlet's unit theorem and the finiteness of class number.

3. The notion of an ideal class is essentially due to Kummer [47b] in the case of cyclotomic fields. In the case of quadratic fields it is closely connected with the equivalence classes of binary quadratic forms over $\mathbb{Z}$ of a given determinant under the action of $SL(2,\mathbb{Z})$, which were studied already by Lagrange [73] and Gauss [01]. We shall establish this relation in Chap. 8.

Ideal classes mod I were introduced by H.Weber [97], and ideal classes in the narrow sense, forming $H_I^*(K)$, by Landau [18b]. Theorem 3.25 is due to them.

The class-number can be also defined in terms of matrices (Châtelet [11], Hurwitz [95b]). There are several relations between matrix theory and the theory of algebraic numbers. On this topic see Bennett [23], Bhandari, Nanda [79], Châtelet [11], Faddeev [74], Latimer, McDuffee [33], Taussky [49], [51], [57], [60], [62], [77a], [80], Taussky, Todd [40]. It has been proved in Bass, Milnor, Serre [67] that for $n \geq 3$ every element of the group $SL_n(R_K)$ can be written as a product of elementary matrices. Under the assumption of GRH Cooke and Weinberger [75] proved the existence of a bound for the number of necessary factors, depending only on n, in the case when K is not imaginary quadratic. This number has been later shown, without using GRH, to be bounded by $(3n^2 - n)/2 + 68\omega(d(K)) - 1$ in all cases (Carter, Keller [83]).

4. The finiteness of the group $H(K)$ (Theorem 3.7) in the quadratic case goes back essentially to Lagrange [73], who studied classes of binary quadratic forms. In the cubic case it was established by Eisenstein [44b], who also used the language of forms. For cyclotomic fields it was proved by Kummer [47b], [56], and the general case is due to Dedekind [71] and Kronecker [82]. We presented the proof of Minkowski [91a]. Other proofs were given in Artin, Whaples [45], Hurwitz [95c], Mahler [64]. A proof in which $H(K)$ is shown to be at the same time a continuous image of a compact group and a discrete group can be found in Cassels, Fröhlich [67].

It is not known, whether every finite Abelian group can serve as $H(K)$ or $H^*(K)$ for suitable field K. In Chap. 8 we shall present a result of S.Chowla [34b] which shows that the answer is negative, if one restricts K to be imaginary quadratic (see Corollary to Proposition 8.24). Chowla's proof is not effective, but Shanks [69] showed that for such fields one cannot have $H(K) = C_p \oplus C_p$ with $p = 5$, 7 or 11. It is known (Perret [99]) that every finite Abelian group is isomorphic to $H(K_S)$ for suitable K and S. For the structure of the group of ray classes see Stevenhagen [94b], H.Cohen, Diaz y Diaz, Olivier [98a].

Fröhlich [62a] and Hasse [69d] showed that every finite Abelian group A is a homomorphic image and also a subgroup of $H(K)$ for infinitely many fields K (cf. Frey, Geyer [72]). This was strengthened by Cornell [71], who proved that one can always choose K to be cyclotomic. It was shown in Sonn [83] that every such A is a direct summand of $H(K)$ infinitely often, and in Yahagi [78] it has been proved that if A is a p-group, then it is the Sylow p-subgroup of a $H(K)$ for a suitable cyclic $K/\mathbb{Q}$. See also Gerth [75b], Iimura [81a], Yamamura [91].

5. Lemma 3.8 is due to Minkowski [91a] (cf. Minkowski [96a], [07]). If we denote by $C(r_1, r_2)$ the lower bound of numbers C with the property that for every field of signature $[r_1, r_2]$ each class of $H(K)$ contains an ideal with norm not exceeding $C|\sqrt{d}|$, then for sufficiently large $r_1 + 2r_2$ one has

$$C(r_1, r_2) < a^{-r_1/2} b^{-r_2},$$

with $a = 50.7$ and $b = 19.9$, as shown by Zimmert [81]. For an improvement in the case of small degree see Maza [02].

For cubic fields Minkowski's bound was improved in Delaunay, Faddeev [40], and for certain quartic fields in Lubelski [60] (see also Lemmermeyer [97b]). On the other hand for quadratic fields K we have

$$\max_{X \in H(K)} \min_{I \in X} N(I) \geq B \frac{\sqrt{D}}{\log D \log \log^T D},$$

where $D = |d(K)|$, and B, T are positive numbers, depending only on $h(K)$ (Anfert'eva, Chudakov [64], [70]). Generalizations of Lemma 3.8 to other base fields were given in Kuroda [62], Lakein [69], Mordell [69], Nymann [67].

An algorithm for the computation of h for real quadratic fields with expected running time of order $O(d^{1/5+\epsilon})$ gave Srinivasan [98]. Unfortunately, the involved constant is not effective.

The exponent of the class-group of pure cubic number fields of the form $Q(\sqrt[3]{1+a^3})$ and $Q(\theta_a)$ (with $\theta^3 = a\theta^2 + 1$) was considered by Louboutin [99c], who proved that under *GRH* it tends to infinity in both cases and determined all fields $\mathbb{Q}(\sqrt[3]{m^3+1})$ with exponent ≤ 2. All fields $\mathbb{Q}(\sqrt[3]{m^3+r})$ with $m \geq 1$, $r|3m^2$ and $h = 1$ were found in Byeon [96]. A table of the 2-ranks of $H(K)$ for non-cyclic cubic fields with $|d(K)| \leq 10^{25}$ was computed in Schneiders [97] (there is only one such field with 2-rank equal to 7).

A sufficient condition for $h = 1$ in totally real fields gave Byeon [01a].

The class numbers of quintic fields with small discriminants were computed in Pohst, Wildanger [98].

A bound for the smallest norm of an element in a residue class mod I was obtained by Davenport [52] (cf. Egami [80], Rieger [58d], Tatuzawa [73a]).

6. Algebraic units appears first in Gauss [32] in the case $K = \mathbb{Q}(i)$. The general notion was worked out at the same time as that of an integer. The main result of the theory of units, Theorem 3.13, was proved by Dirichlet[1] [46] for the units of $\mathbb{Z}[a]$, with an integer a, however his argument can be easily extended to cover the general case. Earlier, in [40], he showed that in case $r_1(K) \geq 1$ there are infinitely many units, and in [41c] the cubic case was treated (cf. Bachmann [64]). In the special case $K = \mathbb{Q}(\zeta_p)$, with prime p, Theorem 3.13 was proved independently by Kronecker [45a], [83],[84]. Other proofs can be found in Artin, Whaples [45], Hermite [50], Iwasawa [53a], Minkowski [96a], van der Waerden [28]. An elementary proof in the case of pure cubics appears in Christofferson [57].

The more general Theorem 3.12 was first published in Chevalley [40]. For another proof see Mahler [64], and for generalizations and analogues see Bass [66], May [70], Roquette [57], Samuel [66].

[1] According to Minkowski the idea of the proof occurred to Dirichlet during an Eastern concert in the Sistine Chapel.

An effective procedure determining a system of fundamental units is given in H.Cohen [93] and Pohst, Zassenhaus [89]. See also Avanesov [79], Benson, B.T.Weber [73], Pohst [94], Pohst, Weiler, Zassenhaus [82], Pohst, Zassenhaus [77], [82], Rudman, Steiner [78],

The last part of Proposition 3.11 is due to Ore [24]. The Corollary to Lemma 3.15 gives in the case of totally real K certain information about the action of the unit group on R^n (with $n = [K : \mathbb{Q}]$) defined by

$$u\langle x_1, \ldots, x_n\rangle = \langle F_1(u)x_1, \ldots, F_n(u)x_n\rangle$$

for $u \in U(K)$. This induces an action of $U^+(K)$ on the cone in R^n consisting of elements with non-negative coordinates. The fundamental domain for this action was determined by Shintani [76b], who in [81] carried out this construction for fields of arbitrary signature.

Theorem 3.13 shows that the group $U(K)$ is finitely presented. Zassenhaus [72] obtained the same assertion for the group of units of any commutative ring with unit, whose additive group is isomorphic to $\mathbb{Z}^n$ with some n. Skolem [48] deduced from Theorem 3.13 that the multiplicative group K^* is the direct product of $E(K)$ and a free Abelian group with denumerably many free generators. This was extended by Schenkman [64], who proved that the multiplicative group of the field generated by all algebraic numbers of degree $\leq n$, is a direct product of cyclic groups. This implies that every multiplicative group generated by a set of algebraic numbers of bounded degree is a product of cyclic groups. For the case of infinite extensions see Iwasawa [53c], Horie [90]. It has been proved in Brandis [65] (see also Brown [87], Samuel [71]) that if $K \subset L$ and $K \neq L$, then the factor-group L^*/K^* cannot be finitely generated.

If $R \subset S$ are orders in R_K, then the index $[U(S) : U(R)]$ is finite. A bound for this index was given in Wolfskill [95],[97].

7. *Units of real quadratic fields.* It is clear that every result about the Pellian equation $X^2 - DY^2 = \pm 4$ gives some information about units in real quadratic fields. This permits us to treat Lagrange [66] as the author of Theorem 3.13 in this case. For a survey of older results on the Pellian equation the reader should refer to Chap. XII of Dickson [19].

For certain classes of fields explicit formulas for the fundamental unit are known. The first such formulas were obtained by Richaud [66] and rediscovered later by Degert [58]. They considered square-free $D = n^2 + r$ ($-n < r \leq n$ and $r|4n$) and showed that the number

$$\epsilon = \begin{cases} n + \sqrt{D} & \text{if } r = \pm 1, D \neq 5, \\ (n + \sqrt{D})/2 & \text{if } r = \pm 4, \\ (2n^2 + r + 2n\sqrt{D})/|r| & \text{if } r \neq \pm 1, \pm 4 \end{cases}$$

is the fundamental unit of the field $\mathbb{Q}(\sqrt{D})$. Such fields are now called *Richaud-Degert fields*. For similar results see Azuhata [84], Bernstein, Hasse

[75], Kutsuna [74], Nakahara [70], Neubrand [81], Nordhoff [74], Uehara [83], Yokoi [68a], [70a].

The first tables of minimal solutions of Pellian equations were published by Legendre [98], Degen [17], Bickmore [93], Whitford [12], covering jointly the range $[2, 1700]$ (see Lehmer [26] for a list of errors). With the advent of computers the determination of such solutions as well as of fundamental units of quadratic fields became an easy task, at least for not too large values of D.

For asymptotical results dealing with fundamental solutions of the Pellian equation the reader should consult Hooley [84].

Several authors have studied the sign of the norm of the fundamental unit ϵ of a real quadratic field K, trying to express it in terms of various invariants of K, since it dependence on the parity of the period of the continued fraction given in Theorem 3.19 is not very useful. A quick algorithm for the determination of this sign appears in Lagarias [80a]. In a series of papers Rédei ([35], [38], [53]) used class-field theory to deduce a necessary and sufficient condition for $N_{K/\mathbb{Q}}(\epsilon) = -1$ (cf. Morton [79]). For various sufficient or necessary conditions see Brown [83], Epstein [34], Jensen [62], v.Lienen [78], Pall [69], Perott [88], Pumplün [68], Scholz [35], Tano [89].

An interesting relation between signatures and residue classes mod 4 of units, and, more generally, of integers a, prime to 2, was discovered by Lagarias [78]. He observed that if $d(K)$ is a sum of two squares, then a mod 4 determines the signature of a, Sunley [79] proved that the same holds for all totally real fields K with odd $h^*(K)$, and Lagarias [80b] proved that a totally real field K has this property if and only if the 2-ranks of $H(K)$ and $H^*(K)$ coincide. Cf. Haggenmüller[82].

Recall that the n-th *Bernoulli number* B_n is defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

It has been established by Ankeny, Artin and Chowla [52] that if $p \equiv 1 \pmod 4$ is a prime, $(T + U\sqrt{p})/2$ is the fundamental unit and h the class-number of $Q(\sqrt{p})$, then

$$\frac{Uh}{T} \equiv B_{(p-1)/2} \pmod p,$$

and they conjectured that $p \nmid U$. This has been checked for $p < 10^{11}$ (van der Poorten, te Riele, Williams [01]). It is known that it is equivalent to $p \nmid B_{(p-1)/2}$ (Mordell [60a] for $p \equiv 5 \pmod 8$, Ankeny, Chowla [62] in the remaining case). Generalizations of the Ankeny-Artin-Chowla conjecture were given in Jakubec [96b], H.Lang [73b], Mordell [60a], Slavutskii [65a].

It has been observed in Sprindzhuk [74a] that if $E(x)$ denotes the number of fundamental units ϵ of all real quadratic fields, lying in the interval $(1, x)$, then

$$E(x) = 2 \sum_{k=1}^{[\log x]} \mu(k) x^{1/k} + O(\log x).$$

8. *Cubic units.* A theory of units in cubic fields was outlined by Hermite in a letter to Jacobi (Hermite [50]). His ideas were used for the actual construction of units by Zolotarev [69] in the case of pure cubic fields. The general case was treated by Voronoi [96]. See Delaunay, Faddeev [40] for a presentation of Voronoi's approach. Cf. also Brentjes [81]. In certain cases one can obtain fundamental units with the Jacobi-Perron algorithm, which goes back to Jacobi [68] and Perron [07]. On this subject see Bernstein [71].

Other methods, algorithms and explicit formulas for certain classes of cubic fields may be found in Appelgate, Onishi [82], Arwin [29], Avanesov, Billevich [81], Bergmann [66b,c], Berwick [13], [32], [34], Billevich [56], Brunotte, Halter-Koch [79], [81a], Bullig [36], [38], Cusick [82], [84b], Endô [78], Godwin [60], [84], Güting [77], Hasse [48a], Ishida [73], Minkowski [96b], Morikawa [74], Rudman [73], Steiner, Rudman [76], Stender [69], [72], [75], [77], Vel'min [51], Vulakh [02], Watabe [83], H.C.Williams [76], [80], [81b], Williams, Cormack, Seah [80], Yokoi [74]. In Thomas [79] and Grundman [95] units of subrings of R_K were constructed.

Tables of cubic fields were provided by Llorente, Quer [88b] and Fung, Williams [90], covering fields with discriminants in the range $[-10^6, 10^7]$.

9. Methods of finding fundamental units in various classes of quartic fields were given in Amara [81], Berwick [32], Frei [81a], [82], Hasse [48a], Kuroda [43] (cf. Kubota [56b]), Levesque [81], [82], Nagell [62], R.Scharlau [80], A.Stein [27], Stender [73], [75], [77], [78], [83], Wada [66], and for sextic fields in Bergmann [65], Frei [81b], Hasse [48b], Iimura [80], Mäki [80], Nakamula [79], Setzer [78], Stender [74], [75], [77], [78].

For other classes of fields see Bernstein [75a,b], [77], [78a,b], H.Cohn [76], Frei, Levesque [79], [80], Greiter [80], Halter-Koch [75], [82], Halter-Koch, Neubrand [78], Oozeki [78], [79], Stender [74],.

10. Proposition 3.20 is due to Remak [52]. Several other characterizations of CM-fields were given in Győry [75]. Theorem 3.21 was in the case $K = \mathbb{Q}(\zeta_p)$ with prime p stated by Kummer [50a] and proved by him in [51]. Another proof in this case appears in MacCluer, Parry [75]. The general case is due to Latimer [34] (cf. M.J.Weiss [36]). Theorem 3.22 is due to Dénes [51] and the presented proof appeared in MacCluer, Parry [75]. The assumption of normality in this theorem is not necessary, as shown in Parry [75a]. Lemma 3.23 for $K = \mathbb{Q}(\zeta_p)$ was proved by Kummer [51]. The Galois groups of normal closures of CM-fields were considered by Dodson [84], [86], who observed that the theorem of Shafarevich [54] on solvable groups implies that every solvable finite group, containing an element of order 2 in its center, is the Galois group of a CM-field.

Theorem 3.25 shows that a real field K has totally positive fundamental units if and only if $h^*(K) = 2^{r_1-1}h(K)$. See Armitage, Fröhlich [67], Taylor [75]. For the Corollary 4 to Theorem 3.25 see Kaplan [74]. A sufficient condition for the existence of units of all signatures was given by Neumann [77]. By the Corollaries 2 and 3 to Theorem 3.25 this occurs for a totally real field if and only if $U^+(K) = U^2(K)$. For the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_m)$ (with $m \not\equiv 2 \pmod 4$) this happens in the case when m is a prime power (Garbanati [76]). For prime m this is due to Kummer [70] and for $m = 2^k$ to H.Weber [96b]. Cf. Armitage, Fröhlich [67], Hasse [52a], Hughes, Mollin [83].

The results of Berwick [32] imply that every totally real cubic field has a fundamental system of units formed by PV-numbers, and Zlebov [66] showed that the same applies to all real fields. Cf. Brunotte, Halter-Koch [81b].

11. Theorem 3.26 is due to Minkowski [00] (in the special case $K = \mathbb{Q}(\zeta_p)$ it appears already in Kummer [51]). It was later extended by Herbrand [30b], [31b] to relative extensions. A simplified proof of Herbrand's result was given by Artin [32a], and a further generalization appears in Lednev [39]. It has been proved by Latimer [34] that a cyclic field has a strong Minkowski unit if and only if certain ideal in a matrix ring is principal. Theorem 3.28 appeared explicitly first in Zeinalov [65] (for $p = 3$ this was shown in Delaunay, Faddeev [40]), but it lies hidden already in Latimer [34]. Brumer [69] proved that it suffices to assume in it that all ideals of norm $h(K)$ in $\mathbb{Q}(\zeta_p)$ are principal. See Gillard [80a] for a generalization.

Marko [96] established the existence of Minkowski units in real cyclic fields of degrees 4, 6 and 10, but note that a real cyclic quartic field may not have a strong Minkowski unit, as the example $K = \mathbb{Q}(\sqrt{65 + 2\sqrt{5}}\,)$ (Bouvier, Payan [75]) shows. It was proved by N.Moser [83] that every imaginary dihedral extension of $\mathbb{Q}$ of degree $2p$ (with prime p) has a Minkowski unit. We shall prove her result in Chap. 7 (see Theorem 7.25). For other classes of fields no such complete results are known. Cf. Latimer [34], N.Moser [79a], Payan [81], M.J.Weiss [36].

The action of Galois group G on $U(K)$ was studied for certain Abelian groups in Bouvier, Payan [75], [79], Duval [81], Hasse [48b], Pollaczek [29], Setzer [78], [80b], and for some non-Abelian groups in Halter-Koch [78a], Jaulent [79], N.Moser [78], [79a,b], Nakamula [82a]. Most of theses papers contain conditions for the existence of a Minkowski unit. For the existence of a conjugated system of generators in $U^+(K)$ see Hasse [48a], Morikawa [68].

A new approach to study the Galois structure of the unit group was introduced by Chinburg [83b], [84], [89] and the resulting development was subsumed in the book of A.Weiss [96]. For further progress see Burns [95b], Burns, Holland [97], Greither [96] (where one of Chinburg's conjectures was establishes for Abelian fields with odd conductor), Ritter, A.Weiss [97].

12. Denote by K_n the n-th cyclotomic field, i.e. $K_n = \mathbb{Q}(\zeta_n)$, with ζ_n being an n-th primitive root of unity. If p is an odd prime, then the subgroup of $U(K_p)$ generated by all units of the form $(\zeta_p^a - 1)/(\zeta_p^b - 1)$ with $1 \leq a, b \leq p-1$ is called the group of *cyclotomic units*. We shall denote it by $C(K_p)$. It has been shown by Kummer [50a,b], [51] that the index of $C(K_p)$ in $U(K_p)$ is equal to $h(K_p^+)$ (cf. Hilbert [97, Satz 142], S.Lang [78], [82], Washington [82]). A way of computing the minimal polynomial for cyclotomic units was shown in Gurak [82].

Cyclotomic units were defined also in other Abelian fields and this led to an exact analogue of Kummer's index formula for cyclotomic fields K_{p^n}, when p^n is a prime power. There are actually two definitions of cyclotomic units for Abelian fields which agree in the fields K_{p^n}. According to the first, the group of cyclotomic units $C_0(K)$ of an Abelian field K equals the intersection of $U(K)$ with the group generated by roots of unity of order f, where K_f is the minimal cyclotomic field containing K (such field exists by the Kronecker-Weber theorem which we shall prove in Chap. 6) and by $1 - \zeta_f^a$ $(2 \leq a \leq f-1)$.This definition is commonly used for cyclotomic fields. The second definition, used for non-cyclotomic Abelian fields, states that the group $C(K)$ of cyclotomic units is the intersection of $U(K)$ with the group generated by -1 and all numbers of the form $N_{K_n/L_n}(1 - \zeta_n^a)$ with $n = 2, 3, \ldots$, $n \nmid a$, and $L_n = K \cap K_n$. The index of $C(K)$ and $C_0(K)$ in $U(K)$ has been computed by Sinnott [78], [80] (see also Dohmae [97], Kučera [97]). In Hasse [52a] still another definition of the group of cyclotomic units was used, leading to a finite index only in the case of K_{p^n}, in which case it coincided with $C(K_{p^n})$. Its rank has been computed in Feng [82a].

For the structure of the p-Sylow group of $U(K)/C(K)$ in case when K is real and $p \nmid [K : \mathbb{Q}]$ see Gillard [77], G.Gras [77a,b], Greenberg [75], Mazur, Wiles [84]. The conjecture of G.Gras [77b] that in this case the p-components of the groups $U(K)/C(K)$ and $H(K)$ have isomorphic compositions series has been established by Wiles [90a] (cf. Kolyvagin [90], Kuzmin [96]).

Analogues of cyclotomic units in Abelian extensions of imaginary quadratic fields are provided by *elliptic units*, defined with the use of singular values of modular functions. They were introduced by Robert [73], but in special cases they appeared already in Fueter [10], Siegel [61] and Novikov [67]. For their properties and applications see Coates, Wiles [78], Gillard [79a,b,c], [80a,b], Gillard, Robert [79], Kersey [80], Kubert, Lang [79], [81], Nakamula [82b], [85a,b], [89], Robert [78], [79].

13. If $a, b \in R_K$ generate the unit ideal, then for infinitely many integers x (not necessarily lying in K) the number $ax + b$ is a unit (see Chabauty [38]). A similar result holds also for polynomials in several variables over $\mathbb{Z}$ (Skolem [35]). Cf. Cantor, Roquette [84], Jacobsthal [13], Dade [63], Lagarias, Lenstra [81].

It has been shown by Cooke, Weinberger [75] (see also Lenstra [77b]) that if K is not imaginary quadratic, then *GRH* implies that for infinitely many

prime ideals $\mathfrak{p}$ every non-zero residue class mod $\mathfrak{p}$ contains a unit, i.e. one has $\Phi(I) = \psi(I)$, In the case of real Abelian fields this has been established in Narkiewicz [88] unconditionally, with possible exception of at most two fields of degree ≤ 3. The value of $\Phi(I)/\psi(I)$ was studied under the assumption of *GRH* for real quadratic fields in Chen, Kitaoka, Yu [00] (cf. Ishikawa, Kitaoka [98]), and for cubic fields in Kitaoka [01].

14. A solution of the equation

$$a_1x_1 + \cdots + a_nx_n = b \tag{3.7}$$

with $b \neq 0, a_1, \ldots, a_n$ is called non-trivial, if none of the subsums of the left-hand side vanishes. In the case $n = 2$ and $b = 1$ it follows from results of S.Lang [60] and Lewis, Mahler [60] that there are only finitely many solutions of (3.7), and an explicit bound for the number of solutions, independent of a_1, a_2, was in this case (also for S-units) obtained in Evertse [84], (cf. Beukers, Schlickewei [96], Bombieri, Mueller, Poe [97], Evertse, Győry [85]). Later it has been shown that a similar bound holds for non-trivial solutions in the case of arbitrary n and non-zero b (Schlickewei [90]. Cf. Bugeaud, Győry [79b], [96a], Evertse, Győry [88a], Evertse, Schlickewei [02], Evertse, Schlickewei, W.M.Schmidt [02], van der Poorten, Schlickewei [91]). The obtained bounds are exponential in $\#S + [K : \mathbb{Q}]$, and it is known that there cannot exist a polynomial bound (Erdős, C.L.Stewart, Tijdeman [88], Evertse,Moree, C.L.Stewart, Tijdeman [03]). However, in the case $n = 2$ for the majority of numbers a_1, a_2, b there are at most two solutions (Evertse, Győry, C.L.Stewart, Tijdeman [88a]) (cf. Győry [79b]). Algorithms for finding all non-trivial solutions in case $n = 2$ were given in Smart [99] and Wildanger [00].

Bounds for the number of non-trivial solutions of (3.7) in the case, when $a_1, \ldots, a_n$ are arbitrary complex numbers and the x_i's are roots of unity were obtained in Schlickewei [96] and Evertse [99]. For the case of rational or algebraic coefficients a_i see Conway, Jones [76], Mann [65], Schinzel [88], Zannier [89].

Units $u \in R_K$ for which $1 - u$ is also a unit were called *exceptional units* by Nagell [69b]. There are only finitely many such units in any K, since they are solutions of (3.7) in the case $n = 2$. This follows already from a result of Siegel [21a; Satz 10] (cf. Nagell [64b]). Exceptional units in quadratic, cubic and certain quartic fields were determined in Nagell [59], [60], [64b], [69a,b] (cf. Chowla [61a]). Cubic fields containing exceptional units were studied in Ennola [91] and for quartic fields see also Niklasch, Smart [98]. Upper bounds for the number of exceptional units in a given field were obtained in Győry [73], Evertse [84] and Niklasch [97]. It has been proved in Nagell [69a] that for every $n \geq 5$ there exists a field of degree n having at least $6n - 9$ exceptional units. Fields with many exceptional units were considered in Grant [96]. For a survey on linear unit equations see Evertse, Győry, C.L.Stewart, Tijdeman [88b].

Other unit equations were considered in Chabauty [37], Ennola [73b], [75b,c], Grossman [76], [77], Kostra [94], Loxton [74b], Mahler [50], Mordell [63], Newman [71], [74a], [90], [93], Pethő [93], Siegel [21a], Silverman [95], Watabe [82].

Define $L(K)$, (the *Lenstra constant*) (Lenstra [77a]) of K, as the largest integer M such that there exist M distinct integers of K, whose all non-zero differences are units. Since these integers must be distinct mod 2 it follows that if K is of degree n, then $L(K) \leq 2^n = N_{K/\mathbb{Q}}(2)$. It has been shown in Győry [95] that the maximal number of units of degree n, whose all non-zero differences are also units, does not exceed $\exp(36n^{2n+5})$.

15. *Evaluations of the regulator.* The first general upper bound for $R(K)$ was obtained by Landau [18d], who proved

$$R(K) = O\left(\sqrt{D}\log^{n-1} D\right),$$

where $n = [K : \mathbb{Q}]$ and $D = |d(K)|$ (see Corollary 4 to Theorem 7.3). See also Landau [18a], Remak [31], Siegel [69a]. For a similar result dealing with the class-number and regulator of orders see Sands [91].

Evaluations of the product $R(K)h(K)$ will be considered in Chap. 8.

Lower bounds for $R(K)$ were first established by Remak [31], [32], [52], [54]. who showed that for totally real K one has $R(K) \geq 10^{-3}$. A substantial improvement in this case was made by Pohst [77], who got $R(K) \geq 0.315$, and, for sufficiently large $n = [K : \mathbb{Q}]$, $R(K) \geq \exp(4n/5)$. For cubic fields see Cusick [84a]. For arbitrary K one has $R(K) \geq 0.2052\ldots$ (Friedman [89]) and this bound is optimal. Quartic fields were considered in Cusick [84a] and Nakamula [96]. In the general case one has

$$R(K) \geq c_1(n)\left(c_2(n)\log(|d(K)|)\right)^{r-r'},$$

where $r = r(K)$, r' is the maximal unit rank of proper subfields of K and $c_1(n), c_2(n)$ are positive. This was established by Silverman [84], who conjectured that the exponent of the logarithm in this formula is optimal (cf. Uchida [94]. For lower bounds for $R(K)$ depending only on the signature of K see Zimmert [81], Skoruppa [93], Slavutskii [92]. The last author obtained

$$R > 0.0001w\exp(0.81r_1 + 0.57r_2),$$

with $w = \#E(K)$.

For lower bounds for the ratio $R(L)/R(K)$ in case $K \subset L$ see Bergé, Martinet [89] and Costa, Friedman [93].

Upper bounds for the number of fields of a given degree, satisfying $R(K) \leq x$ were obtained in Sprindzhuk [74b].

Regulators for quintic fields of small discriminants have been computed in Pohst, Wildanger [98].

For real quadratic fields the regulator equals $\log \epsilon$, where $\epsilon > 1$ is the fundamental unit. It has been established by Lavrik [70] that for every $\delta > 0$ and sufficiently large $d = d(K)$ one has

$$\log \epsilon \leq \frac{1}{h(K)}(.263 + \delta)\sqrt{d} \log d.$$

Earlier Y.Wang [64] proved $\log \epsilon \leq (.25 + \delta)\sqrt{d} \log d$, which is slightly better than Lavrik's result in the case $h(K) = 1$. For earlier bounds see Chowla [64], Hua [42], Perron [14], Remak [13], Schmitz [16] and Schur [18b]. See also J.H.E.Cohn [77], Stephens [72], Takaku [71], Yokoi [70b]. On the other hand, for infinitely many d one has $\log \epsilon > B \log^4 d$ with a certain positive B (Halter-Koch [89]. See also Reiter [85], Yamamoto [71]).

16. Proposition 3.33 in the case of the field $\mathbb{Q}(i)$ goes back to Gauss [32]. The Euclidean algorithm can be used, as in the case of rational integers. to determine the greatest common divisors of two integers. The number of steps in Euclidean algorithm in norm-Euclidean imaginary quadratic fields was dealt with in Baldisseri [75] and Rolletschek [86].

Dickson [23a] showed that real quadratic fields K with $d(K) = 5, 8, 12$ and 13 are norm-Euclidean and asserted that there no other such fields. This was shown to be false by Perron [32], who proved Theorem 3.31, and showed that $\mathbb{Q}(\sqrt{44})$ also is norm-Euclidean. Later the list of real quadratic norm-Euclidean fields was extended to contain also fields with discriminants 33, 37, 41, 57, 73, and 76 (Berg [35], Hofreiter [35], Oppenheim [34], Rédei [41], Remak [34]), A uniform proof that all these fields are norm-Euclidean was given in Varnavides [52].

The finiteness of the set of norm-Euclidean real quadratic fields was established in the case $Q(\sqrt{p})$ with prime p by Erdős and Chao Ko [38], and by Heilbronn [38a] in the general case. The final step in showing that the above list of such fields is complete was made in Chatland, Davenport [50], after preliminary work of several authors, who covered various special cases. It has been observed in Arpaia [68] that every norm-Euclidean real quadratic field contains a subring which is not norm-Euclidean.

Davenport [49], [50a] proved that there are only finitely many norm-Euclidean complex cubic fields, all satisfying $|d(K)| \leq 64 \cdot 10^{26}$. He also proved (Davenport [50b]) the same assertion for totally complex quartic fields. They all satisfy $|d(K)| \leq 230\,202\,117$ (van der Linden [84b]). The finiteness of the set of norm-Euclidean cyclic cubic fields was established in Heilbronn [50] and this was generalized in Heilbronn [51] to cyclic fields of a fixed degree and prime-power discriminant. On the other hand Heilbronn [50] conjectured that there are infinitely many real non-cyclic norm-Euclidean cubic fields. The only norm-Euclidean pure cubic fields are $\mathbb{Q}(\sqrt[3]{D})$ with $D = 2, 3$ and 10 (Cioffari [79]) and there are only finitely many norm-Euclidean pure quartic and quintic fields (Egami [84], Lemmermeyer [89]). For norm-Euclidean cubic

fields see also Cavallar, Lemmermeyer [98], [00]. The maximal real subfields of $Q(\zeta_n)$ are norm-Euclidean for $n = 16$ and $n = 32$ (Cerri [00]).

To find norm-Euclidean fields one usually applies geometrical methods. Lenstra [77a] used them to formulate arithmetical conditions for norm-euclidicity. Lenstra showed that if the Lenstra constant $L(K)$ is large, e,g, it exceeds the Minkowski constant of K, then K is norm-Euclidean. This led to many new norm-Euclidean fields (Lenstra [77a,b], Leutbecher [85], Leutbecher, Martinet [82a,b], Martinet [79a], Mestre [81]). In 1985 one knew 576 such fields (Leutbecher [85]), in 1995 already 743, the largest degree being 12, and Quême [98] proposed a new algorithm for checking the norm-euclidicity, which led to more than 1200 new quartic, quintic and sextic norm-Euclidean fields.

Constructive criteria for euclidicity were given in Rodosskii [80] and Motzkin [49]. If S is a sufficiently large finite set of prime ideals of R_K then the ring K_S is Euclidean (O'Meara [65], Queen [73]). It has been proved in Gupta, Murty, Murty [87] that if K is real of degree n, $\#S \geq \max\{5, 2n-1\}$ and K_S is a principal ideal domain, then it is Euclidean. A similar result holds for complex fields, but one has to assume additionally that K contains sufficiently many roots of unity. If one assumes GRH, then this result is true if $\#S \geq 2$ (Lenstra [77b]). This shows in particular that if K is not imaginary quadratic and $h(K) = 1$, then GRH implies the existence of an Euclidean algorithm in R_K (Weinberger [72a]). If K is a totally real quartic field, then one can obtain this unconditionally, provided that for some prime ideal $\mathfrak{p}$ in R_K every invertible residue class mod $\mathfrak{p}^2$ contains a unit (Clark, Murty [95]) This theorem does not hold for imaginary quadratic fields, as can be shown by the example $\mathbb{Q}(\sqrt{-19})$ (Dubois, Steger [58], Lemmlein [54], Motzkin [49], K.S.Williams [75]).

All Euclidean rings of the form K_S with $\#S \leq 2$ were determined by van der Linden [84a].

A survey of Euclidean fields with an excellent bibliography gave Lemmermeyer [95b].

A variant of of the euclidicity, called *k-stage euclidicity* was introduced by Cooke [76], who proved that if K with $h(K) = 1$ is not imaginary quadratic, then it is k-stage Euclidean for a certain $k = k(K)$, and in Cooke, Weinberger [75] it was proved that under GRH one has $k(K) \leq 4$. For some fields this can be proved without assuming GRH (Clark [96]).

Another generalization of Euclidean algorithm appears in Johnson, Queen, Sevilla [85]: A field K is called *generalized Euclidean*, if for $a, b \in R_K$ with $b \neq 0$ and principal (aR_K, bR_K) there exist $q, r \in R_K$ with $a = qb + r$ and $|N_{K/\mathbb{Q}}(r)| < |N_{K/\mathbb{Q}}(b)|$. They proved that there are only finitely many such fields of the form $Q(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is a prime and showed that for real quadratic fields K with $4|d(K)$, if K is generalized Euclidean then it is also norm-Euclidean, except for $d(K) = 40$.

Theorem 3.34 is in this form due to Hasse [28], and has been rediscovered several times. In the case of rings of integers it was obtained earlier by Dedekind [31] and Rabinowitsch [13].

EXERCISES

1. Prove that a field K is a CM-field if and only if it is non-real, closed under complex conjugation s, and s commutes with all embeddings of K in $\mathbb{C}$.

2. Call two ideals I, J of R_K strongly equivalent if there exist non-zero $a, b \in R_K$ such that $aI = bJ$ and $N_{K/\mathbb{Q}}(a/b)$ is positive. Prove that the resulting equivalence classes form a group under multiplication, and find a relation between its cardinality and $h(K)$.

3. (Skolem [48]) Prove that the multiplicative group of an algebraic number field equals the product of $E(K)$ and a free Abelian group with denumerably many free generators.

4. Determine the fundamental units of $\mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(\sqrt{19})$.

5. (Yokoi [68a]) Prove that a real quadratic field K has a unit of negative norm if and only if $K = \mathbb{Q}(\sqrt{D})$ where D is not a square, but $D - 4$ is a square of a rational integer.

6. (Kronecker [57b]) Prove that every unit of a cyclotomic field K can be written as a product of a root of unity and a real unit, which may lie outside K.

7. Let $K/\mathbb{Q}$ be a complex normal extension with Galois group G.

(i) Prove that if $g \in G$ acts trivially on $U(K)/E(K)$, then g is either the unit element of G, or equals the complex conjugation.

(ii) Prove that if the complex conjugation acts trivially on $U(K)/E(K)$, then it lies in the center of G.

(iii) Prove that the complex conjugation acts trivially on $U(K)/E(K)$ if and only if the extension $K^+/\mathbb{Q}$ is normal.

8. (Garbanati [76]) Let $L/\mathbb{Q}$ be real Abelian and let $\mathbb{Q} \subset K \subset L$. Prove that if $U^+(K) = U^2(K)$, then $U^+(L) = U^2(L)$.

9. Let $\mathbb{Q} \subset K \subset L$ and assume that $L/\mathbb{Q}$ is Abelian. Prove that if $Gal(K/\mathbb{Q})$ is isomorphic with the 2-Sylow subgroup of $Gal(L/Q)$, then

$$N_{L/\mathbb{Q}}(U(L)) = N_{K/\mathbb{Q}}(U(K)).$$

10. Prove that an irreducible monic polynomial $f \in \mathbb{Z}[X]$ is the minimal polynomial of an exceptional unit if and only if $|f(a)| = 1$ for $a = 0, 1$.

11. (Nagell) (i) Prove that if the field K des not contain ζ_3, then the number of exceptional units in K is divisible by 6.

(ii) Determine all exceptional units in quadratic fields.

(iii) Prove that if K is a complex cubic field which has exceptional units, then either $d(K) = -23$, or $d(K) = -31$.

(iv) Prove the existence of infinitely many cubic real fields having exceptional units.

12. Prove that the Lenstra constant of a field of degree n cannot exceed 2^n.

13. Determine the Lenstra constant for quadratic fields.

14. Prove that for every n there exists a field of degree n in which there exists a unit u such that all numbers $u+1, u+2, \ldots, u+n-1$ are units.

15. (Dress, Scharlau [82]) Let K be a totally real field. A totally positive number $a \in R_K$ is called indecomposable, if it is not a sum of two totally positive numbers.

(i) Prove that up to multiplication by a totally positive unit, there are only finitely many indecomposable numbers in R_K.

(ii) Determine the maximal norm of an indecomposable element in a real quadratic field.

4. Extensions

4.1. The Homomorphisms of Injection and Norm

1. This chapter is devoted to the connections between arithmetic in an algebraic number field K and its finite extension L/K. Such an extension is called traditionally an *absolute extension* if $K = \mathbb{Q}$, and is called a *relative extension* if $K \neq \mathbb{Q}$. The same applies to other notions which will arise in the sequel, and so we shall speak about, say, a *relative discriminant* of an extension, whereas by the *absolute discriminant* we shall mean the discriminant $d(K)$, defined in Chap. 2.

The fundamental results of the theory can be proved in a more general setting, and in this chapter we shall work with an arbitrary Dedekind domain R having K for its field of quotients, L will be a finite separable extension of K, and S will denote the integral closure of R in L. We assume also that the domain R has the (FN)-property. By Theorem 1.20 the ring S is also a Dedekind domain, and S shares the (FN)-property. We shall denote by $G(K)$ and $G(L)$ the groups of fractional ideals of R and S, respectively, and by $I(K)$, $I(L)$ the semigroups of non-zero integral ideals, i.e., of ideals of R and S in the usual sense. In the sequel the zero ideal will be disregarded, and in particular when speaking about prime ideals we shall have in mind only non-zero prime ideals.

Our aim is to describe the relations between $G(K)$ and $G(L)$, and, in particular, we shall deal with two maps defined in a canonical way – the injection map from $G(K)$ to $G(L)$ and the norm map acting in the opposite direction.

We start with the injection map $i_{L/K} : G(K) \longrightarrow G(L)$, defined for $A \in G(K)$ by

$$i_{L/K}(A) = AS.$$

One sees immediately that $i_{L/K}(A)$ is the smallest S-module containing A. It is also clear that this map preserves inclusion and maps principal ideals into principal ideals. Moreover the equality $ABS = (AS)(BS)$ shows that it is a homomorphism.

Proposition 4.1. *The injection map $i_{L/K}$ is a monomorphism, mapping $I(K)$ into $I(L)$.*

Proof : Note first that one has $S \cap K = R$. In fact, the inclusion $R \subset S \cap K$ is obvious, and since every $a \in S \cap K$ is integral over R and lies in K, hence $a \in R$. If now $i_{L/K}(A) = S$, then $SA = S$, whence $R = S \cap K = SA \cap K \supset A$, and so A must lie in $I(K)$. But $i_{L/K}(A^{-1}) = S^{-1} = S$, and we may repeat the last argument to obtain $A^{-1} \in I(K)$. This can happen only if $A = R$, and so the kernel of $i_{L/K}$ is trivial.

If $A \in I(K)$, then $A \subset R$, thus $i_{L/K}(A) \subset i_{L/K}(R) = S$, whence $i_{L/K}(A) \in I(L)$. □

This proposition allows us to treat every ideal of R as an ideal of S, if we identify A and $i_{L/K}(A)$. This idea can be extended so as to make it possible to treat ideals belonging to integral closures of R in various finite extensions of K *in abstracto*, without referring to a particular extension. Observe first that if M/L and L/K are finite separable extensions, then $i_{M/K} = i_{M/L} \circ i_{L/K}$. Now consider the system of groups $\{G(L)\}$, where L runs over all finite separable extensions of a fixed field K, which is the field of quotients of a Dedekind domain R, and $G(L)$ is the group of fractional ideals attached to the integral closure of R in L. This system can be partially ordered by $G(L) \prec G(M)$ holding if and only if $L \subset M$, all fields concerned being subfields of a fixed algebraic closure of K. Since the maps $i_{M/L}$ are compatible with this ordering, we may consider the direct limit G of the system $\{G(L), i_{M/L}\}$. The elements of G are fractional ideals of all fields L which are finite separable extensions of K, two such ideals, say $A \in G(L)$ and $B \in G(M)$ being regarded as equal if and only if there is a common extension N of the fields L and M such that $i_{N/L}(A) = i_{N/M}(B)$. The most important case, at least for us, is the one arising when we take $K = \mathbb{Q}$ and $R = \mathbb{Z}$ and consider all finite extensions of the rationals contained in $\mathbb{C}$.

Let us return to the injection map. If $\mathfrak{p}$ is a prime ideal in R, then there is no need for the ideal $i_{L/K}(\mathfrak{p})$ of S to be prime. However, we can always write

$$i_{L/K}(\mathfrak{p}) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{4.1}$$

where the $\mathfrak{P}_i$'s are prime ideals of S and the exponents e_i are positive rational integers. We shall say that the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ *lie above* $\mathfrak{p}$ (and $\mathfrak{p}$ *lies below* each of them), and the exponent e_i will be called the *ramification index* of $\mathfrak{P}_i$ and denoted by $e_{L/K}(\mathfrak{P}_i)$. The ideal $\mathfrak{P}_i$ is said to be *ramified* in L/K if $e_{L/K}(\mathfrak{P}_i) > 1$, and *unramified* otherwise. If $e_{L/K}(\mathfrak{P}_i)$ is divisible by the characteristic of the field $S/\mathfrak{P}_i$, then $\mathfrak{P}_i$ is called *wildly ramified* in L/K, and ramified prime ideals which are not wildly ramified are called *tamely ramified*. Finally, if $\mathfrak{P}_i$ is either unramified or tamely ramified, then it is said to be *at most tamely ramified*.

One says also that a prime ideal $\mathfrak{p}$ of R is *ramified* in L/K, if at least one of the prime ideals of S lying above $\mathfrak{p}$ is ramified. Similarly, $\mathfrak{p}$ is called *unramified* resp. *tamely ramified* in L/K if all prime ideals of S above $\mathfrak{p}$ are such.

An extension is called *unramified*, resp. *tamely ramified* (or simply *tame*), if all prime ideals of S are unramified or at most tamely ramified, respectively. Note that an unramified extension is tame by definition.

If L is an algebraic number field and $K \subset L$, then the extension L/K is called *unramified at infinity*, if no real embedding of K in $\mathbb{C}$ can be prolonged to a complex embedding of L. In particular, every extension of a totally complex field is unramified at infinity.

Proposition 4.2. *If $\mathfrak{p}$ is a prime ideal of R, $k = R/\mathfrak{p}$, and $\mathfrak{P}$ is a prime ideal of S, lying above $\mathfrak{p}$, then there is an embedding of k in $S/\mathfrak{P}$, and one has $[S/\mathfrak{P} : k] \leq [L : K]$.*

Proof: It follows from Lemma 1.22 that $\mathfrak{p} = \mathfrak{P} \cap R$, and thus the embedding $R \subset S$ induces an embedding of k in $S/\mathfrak{P}$. If a is an element of S, then with suitable $c_i \in R$ we have

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0,$$

with $n \leq [L : K]$, and therefore the canonical image $\bar{a}$ of a in the residue field $S/\mathfrak{P}$ satisfies

$$\bar{a}^n + \bar{c}_{n-1}\bar{a}^{n-1} + \cdots + \bar{c}_0 = 0,$$

with $\bar{c}_i \in k$, hence the $\deg_k a \leq [L : K]$, and since the field $S/\mathfrak{P}$ is finite, the inequality $[S/\mathfrak{P} : k] \leq [L : K]$ follows. □

The degree $[S/\mathfrak{P} : R/\mathfrak{p}]$ will be denoted by $f_{L/K}(\mathfrak{P})$, and called the *degree of* $\mathfrak{P}$ over the field K.

Proposition 4.3. *If $K \subset L \subset M$, T is the integral closure of S in M and $\mathfrak{p} \subset \mathfrak{P}$ are prime ideals of S and T, respectively, then*

$$e_{M/K}(\mathfrak{P}) = e_{M/L}(\mathfrak{P})e_{L/K}(\mathfrak{p}),$$

and

$$f_{M/K}(\mathfrak{P}) = f_{M/L}(\mathfrak{P})f_{L/K}(\mathfrak{p}).$$

Proof: This is an immediate consequence of the definitions of $e_{L/K}$ and $f_{L/K}$. □

Corollary. *If the extensions L/K and M/L are both unramified, or tame, so is M/K.* □

2. Our subsequent results will concern the relations between the ramification indices and ideal degrees. Although they are true in the most general situation (assuming only finiteness and separability of the extension considered), we shall, for simplicity, prove them only in those cases which are really needed for our purposes. Our assumptions, valid in this chapter, are:

(i) K is a field of zero characteristic, R is a Dedekind domain with quotient field K, L/K is an extension of degree n, and S is the integral closure of R in L.

(ii) The ring R (hence also S) has the finite norm property, and for any ideal I of R we have $N(IS) = N(I)^n$.

(iii) The class numbers of R and S are finite.

To show that all rings R_K satisfy these conditions it remains to establish the following proposition:

Proposition 4.4. *If K is an algebraic number field, L/K is its finite extension of degree n, and I is an ideal of R_K, then $N(IR_L) = N(I)^n$.*

Proof : The ideal $I^{h(K)}$ is principal, so let α be its generator. Corollary to Proposition 2.13 gives $N(I)^{h(K)} = |N_{K/\mathbb{Q}}(\alpha)|$, and therefore

$$\begin{aligned} N(\alpha R_L) &= |N_{L/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(N_{L/K}(\alpha)| \\ &= |N_{K/\mathbb{Q}}(\alpha^n)| = |N_{K/\mathbb{Q}}(\alpha)|^n = N(I)^{nh(K)}. \end{aligned}$$

But $\alpha R_L = I^{h(K)} R_L$ and finally we get $N(I^{h(K)} R_L) = N(I)^{nh(K)}$, and $N(IR_L) = N(I)^n$, as asserted. □

Theorem 4.5. *If $\mathfrak{p}$ is a prime ideal in R and (4.1) is the factorization of $\mathfrak{p}S$ in S, then*

$$e_1 f_1 + \cdots + e_g f_g = n,$$

where $e_i = e_{L/K}(\mathfrak{P}_i)$ and $f_i = f_{L/K}(\mathfrak{P}_i)$.

Proof : Taking norms of both sides of (4.1) we obtain

$$N(\mathfrak{p})^n = N(\mathfrak{p}S) = \prod_{i=1}^{g} N(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{g} N(\mathfrak{p})^{e_i f_i} = N(\mathfrak{p})^{e_1 f_1 + \cdots + e_g f_g},$$

and our assertion follows. □

Corollary 1. *If $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{P}$ lies above $\mathfrak{p}$ in S, then $e_{L/K}(\mathfrak{P})$ and $f_{L/K}(\mathfrak{P})$ do not exceed $[L : K]$.* □

Corollary 2. *There are at most $[L : K]$ distinct prime ideals of S, lying above a fixed prime ideal of R.* □

If $\mathfrak{p}$ is a prime ideal of R such that there is only one prime ideal $\mathfrak{P}$ of S, lying over $\mathfrak{p}$, and moreover $e_{L/K}(\mathfrak{P}) = [L : K]$, then $\mathfrak{p}$ is called *totally*, or *fully*, or *completely ramified* in L/K. If $i_{L/K}(\mathfrak{p})$ is a product of distinct prime ideals of degree one, then we say that $\mathfrak{p}$ *splits* in L/K.

3. In this subsection we assume that our extension L/K is normal and G is its Galois group. If I is a fractional ideal in L and $s \in G$, then $s(I)$ is also a fractional ideal. All fractional ideals obtained in this way from a given I will be called *conjugated to* I. The notion of conjugated ideals has a meaning also in the case when L/K is not normal: let $L_1, \ldots, L_n$ be the images of L under its different embeddings into a fixed algebraic closure of K, and let $s_i : L \longrightarrow L_i$ be the corresponding isomorphisms, leaving K fixed. Now if I is a fractional ideal of L, then $s_i(I)$ is a fractional ideal in L_i, conjugated to I.

In the case of normal extensions one can make the preceding theorem more precise:

Theorem 4.6. *If L/K is normal and $\mathfrak{p}$ is a prime ideal in R, then all prime ideals of S lying above $\mathfrak{p}$ are conjugated, and have the same ramification index e and degree f. Moreover, if g denotes their number, then $efg = [L : K]$.*

Proof : Once we get the equality of all ramification indices and of all degrees, the last assertion will follow immediately from Theorem 4.5. Hence it suffices to show that all prime ideals lying over $\mathfrak{p}$ are conjugated, since then the equality of degrees will be immediate, the corresponding residue fields being isomorphic, and the equality of ramification indices resulting by applying a suitable $s \in G$ to the equality (4.1). In fact, since every element s of G acts as a permutation group on the set $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$, hence if $s(\mathfrak{P}_1) = \mathfrak{P}_i$, then

$$\mathfrak{p}S = s(\mathfrak{p}S) = s(\mathfrak{P}_1)^{e_1} \cdots s(\mathfrak{P}_g)^{e_g},$$

and $e_i = e_1$ follows by unique factorization

So we have to prove that all $\mathfrak{P}_i$'s in (4.1) are conjugated, i.e., the group G acts transitively on the set of prime ideals lying over $\mathfrak{p}$. We shall utilize the finiteness of the class-number h of S. This implies the existence of $a \in S$ such that $\mathfrak{P}_1^h = aS$. Denote by $a_1 = a, a_2, \ldots, a_n$ the conjugates of a over K. Since $a \in \mathfrak{P}_1$, we have also $b = a_1 \cdots a_n \in \mathfrak{P}_1 \cap R = \mathfrak{p}$, hence the principal ideal bS is contained in $\mathfrak{p}S$, and so is divisible by it. This shows that for every fixed $\mathfrak{P}_i$ we get $\mathfrak{P}_i | bS$, and therefore $\mathfrak{P}_i$ divides some $a_j S$. Let s be that element in G which carries a onto a_j. Then

$$s(\mathfrak{P}_1)^h = s(a)S = a_j S \subset \mathfrak{P}_i,$$

and we get $s(\mathfrak{P}_1) = \mathfrak{P}_i$, because both $\mathfrak{P}_i$ and $s(\mathfrak{P}_1)$ are prime ideals. So G indeed acts transitively. □

4. This subsection is devoted to the norm homomorphism, which will be a map from $G(L)$ to $G(K)$, defined for every extension L/K, satisfying our standing assumptions. Let $\mathfrak{P}$ be a prime ideal of S and let $\mathfrak{p}$ be the prime ideal of R which lies below $\mathfrak{P}$. We define

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f,$$

with $f = f_{L/K}(\mathfrak{P})$, and extend the definition of $N_{L/K}$ to the full group $G(L)$ by multiplicativity, i.e., we put

$$N_{L/K}(I) = \prod N_{L/K}(\mathfrak{P})^{a_\mathfrak{P}}$$

for $I = \prod \mathfrak{P}^{a_\mathfrak{P}} \in G(L)$.

Now we state some simple properties of the norm map just defined:

Proposition 4.7. *Let I be a fractional ideal in L.*

(i) If $K = \mathbb{Q}$ and $I \subset S$, then $N_{L/K}(I)$ is the principal ideal generated by $N(I)$.

(ii) If $I \subset S$, then $N_{L/K}(I) \subset R$.

(iii) If $I \subset J$, then $N_{L/K}(I) \subset N_{L/K}(J)$.

(iv) If I, J are ideals of S such that I and $N_{L/K}(J)S$ are relatively prime, then the norms $N_{L/K}(I)$ and $N_{L/K}(J)$ are also relatively prime.

(v) For $I \in G(K)$ we have $N_{L/K} \circ i_{L/K}(I) = I^n$, where $n = [L : K]$.

(vi) For any chain $K \subset L \subset M$ of fields we have

$$N_{L/K} \circ N_{M/L} = N_{M/K}.$$

Proof : (i) It suffices to check the assertion for $I = \mathfrak{P}$, a prime ideal. If $p\mathbb{Z}$ is the prime ideal of $\mathbb{Z}$, lying below $\mathfrak{P}$, then $N_{L/\mathbb{Q}}(\mathfrak{P}) = p^f\mathbb{Z}$ with $f = f_{L/\mathbb{Q}}(\mathfrak{P})$, but obviously we have $N(\mathfrak{P}) = p^f\mathbb{Z}$, and our assertion follows.

(ii) Immediate from the definition of the norm map.

(iii) Follows from (ii) and Proposition 1.13 (i).

(iv) Assume the contrary. Then there is a prime ideal $\mathfrak{p}$ of R dividing both $N_{L/K}(I)$ and $N_{L/K}(J)$. This shows that $\mathfrak{p}S$ divides $N_{L/K}(J)S$, thus $\mathfrak{p}S$ and I are relatively prime, and so no prime ideal lying above $\mathfrak{p}$ occurs in the factorization of I. But this means that $N_{L/K}(I)$ cannot be divisible by $\mathfrak{p}$, a contradiction.

(v) It suffices to consider the case $I = \mathfrak{p}$, a prime ideal. If $i_{L/K}(\mathfrak{p})$ has the factorization (4.1), then Theorem 4.5 gives

$$N_{L/K} \circ i_{L/K}(\mathfrak{p}) = \prod_{i=1}^{g} N_{L/K}(\mathfrak{P}_i)^{e_i} = \mathfrak{p}^{e_1 f_1 + \cdots + e_g f_g} = \mathfrak{p}^n.$$

(vi) Immediate by Proposition 4.3. □

The next proposition shows that one can regard the norm of an ideal as the product of all ideals conjugated to it. This makes the norm mapping of ideals similar to the norm mapping of elements.

Proposition 4.8. *Let $K \subset L$, $[L : K] = n$, let M be the minimal normal extension of K containing L, and let T be the integral closure of R in M. Let also G be the Galois group of M/K, and let H be its subgroup, corresponding to L by Galois theory, thus H is the Galois group of M/L. Moreover let X be a set of representatives of cosets sH of G* mod *H. If now I is a fractional ideal of L, then*

$$N_{L/K}(I)T = \prod_{s \in X} s(IT).$$

In particular, if L/K is normal, then

$$N_{L/K}(I)S = \prod_{s \in G} s(I).$$

Proof : We prove first our proposition in the case when L/K is normal, and it is obviously sufficient to prove it in the case $I = \mathfrak{P}$, a prime ideal. Let $\mathfrak{p}$ be the prime ideal of R lying below $\mathfrak{P}$. According to Theorem 4.6 we may write

$$\mathfrak{p}S = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

with $\mathfrak{P} = \mathfrak{P}_1$. For $i = 1, 2, \ldots, g$ denote by G_i the set of $s \in G$, carrying $\mathfrak{P}_1$ onto $\mathfrak{P}_i$. Clearly G_1 is a group and the G_i's are its cosets, whence we obtain

$$\#G_i = n/g = ef,$$

with $f = f_{L/K}(\mathfrak{P})$. This equality implies in turn

$$\prod_{s \in G} s(\mathfrak{P}) = \prod_{i=1}^{g} \mathfrak{P}_i^{ef} = (\mathfrak{p}S)^f = N_{L/K}(\mathfrak{P})S,$$

as asserted.

In the general case again it suffices to consider $I = \mathfrak{P}$, a prime ideal. Observe that

$$\#X = \frac{\#G}{\#H} = \frac{[M : K]}{[M : L]} = [L : K],$$

and, moreover, $s^{-1}s_1 \in H$ implies $s(\mathfrak{P}T) = s_1(\mathfrak{P}T)$. Hence, using Proposition 4.7 (v), (vi) and the part of our proposition already proved, we get

$$\begin{aligned}\left(\prod_{s \in X} s(\mathfrak{P}T)\right)^{[M:L]} &= \prod_{s \in G} s(\mathfrak{P}T) = N_{M/K}(\mathfrak{P}T)T = N_{L/K}(N_{M/L}(\mathfrak{P}T))T \\ &= N_{L/K}(\mathfrak{P})^{[M:L]}T = (N_{L/K}(\mathfrak{P})T)^{[M:L]},\end{aligned}$$

and this implies our assertion. □

Corollary 1. *The norm $N_{L/K}$ maps principal ideals onto principal ideals. More precisely, if I is a principal fractional ideal generated by $a \in L$, then $N_{L/K}(I)$ is the principal fractional ideal generated by $N_{L/K}(a)$.*

Proof : Using the notation of the proposition we get

$$N_{L/K}(I)T = \prod_{s \in X} s(IT) = \prod_{s \in X} s(aT) = \prod_{s \in X} s(a)T = N_{L/K}(a)T,$$

and Proposition 4.1 shows that $N_{L/K}(I) = N_{L/K}(a)R$ is principal. □

This corollary enables us to present a characterization of ideal norms, which may be used as the definition of the norm map:

Corollary 2. *If I is a fractional ideal of L and $K \subset L$, then $N_{L/K}(I)$ is the smallest fractional ideal of K which contains the set*

$$\{N_{L/K}(a) : \ a \in I\}.$$

Proof : The preceding corollary shows that $N_{L/K}(I)$ contains all norms $N_{L/K}(a)$ for $a \in I$. To prove that these norms generate $N_{L/K}(I)$ consider first the case of integral I, i.e., $I \subset S$. By Corollary 4 to Proposition 1.14 there exist $a, b \in I$ such that $I = aS + bS$ and the ideals bS and $N_{L/K}(aI^{-1})S$ are relatively prime. If we define ideals J_1 and J_2 by $aS = IJ_1$ and $bS = IJ_2$, then $N_{L/K}(aS) = N_{L/K}(I)N_{L/K}(J_1)$ and $N_{L/K}(bS) = N_{L/K}(I)N_{L/K}(J_2)$, but Proposition 4.7 (iv) shows that the norms of J_1 and J_2 are relatively prime, thus

$$N_{L/K}(aS) + N_{L/K}(bS) = N_{L/K}(I),$$

as asserted.

If now I is an arbitrary fractional ideal of L, then we may write it in the form $I = A/aS$ with $a \in R$ and $A \subset S$. In fact, we can write $I = B/bS$ with $B \subset S$ and $b \in S$, but the element $c = N_{L/K}(b)/b$ lies in S and $I = cB/cbS = A/a$ with $A = cB \subset S$ and $a = N_{L/K}(b) \in R$. Having done this, observe that for $x \in I$ we have $x_1 = ax \in A$, and so the fractional ideal generated by all elements $N_{L/K}(x)$ with $x \in I$ coincides with the product of a^{-n} by the smallest fractional ideal containing all elements $N_{L/K}(x_1)$ with $x_1 \in A$. But this product equals $a^{-n}N_{L/K}(A) = N_{L/K}(a^{-1}A) = N_{L/K}(I)$.

□

5. From Corollary 2 to Theorem 4.5 one can deduce an evaluation of $h(K)$ for algebraic number fields K, due to Landau [18a]. Although it is rather simple, no better evaluation valid for all algebraic number fields is known. We start with a simple lemma:

Lemma 4.9. *Let K be an algebraic number field of degree n, and denote by $F(a)$ the number of distinct ideals I of R_K with $N(I) = a$. The function F is multiplicative, i.e., the equality $F(ab) = F(a)F(b)$ holds for relatively prime a, b, and, moreover for every $\epsilon > 0$ one has*

$$F(a) \leq d_n(a) = O(a^\epsilon),$$

where $d_n(a)$ denotes the number of factorizations of the number a into n positive factors, taking into account their ordering.

Proof : The multiplicativity of F is an immediate consequence of the fact that every ideal of norm ab with relatively prime a, b is a unique product of ideals with norms a and b, respectively.

Now let $a = p^r$ be a prime power and let $pR_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, where $\mathfrak{P}_i$'s are prime ideals in R_K. If I is an ideal of norm $N(I) = p^r$, and $\mathfrak{P}$ is a prime ideal dividing I, then by Theorem 1.16 we have $N(\mathfrak{P})|N(I)$, whence $N(\mathfrak{P})$ must be a power of p. Thus $p \in \mathfrak{P}$ and we see that $\mathfrak{P}$ coincides with one of the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. This shows that with suitable $a_i \geq 0$ we have $I = \prod_{i=1}^{g} \mathfrak{P}_i^{a_i}$. It follows that every such ideal I induces a factorization of p^r into g factors:

$$p^r = N(I) = \prod_{i=1}^{g} N(\mathfrak{P}_i^{a_i}),$$

and if J is another ideal of norm p^r inducing the same factorization, then with $b_i \geq 0$ we have $J = \prod_{i=1}^{g} \mathfrak{P}_i^{b_i}$ with $N(\mathfrak{P}_i^{b_i}) = N(\mathfrak{P}_i^{a_i})$ for $i = 1, 2, \ldots, g$, whence $b_i = a_i$ and $I = J$. This shows that $F(p^r) \leq d_g(p^r) \leq d_n(p^r)$, due to Corollary 2 to Theorem 4.5. By multiplicativity the lemma follows, the last evaluation being a standard result in elementary theory of numbers. □

The announced upper bound for $h(K)$ runs as follows:

Theorem 4.10. *If $[K : \mathbb{Q}] = n \geq 2$ is fixed and $D = |d(K)|$, then*

$$h(K) = O(\sqrt{D} \log^{n-1} D).$$

Proof : By Lemmas 3.8 and 4.9 we have

$$h(K) \leq \sum_{a \leq c(K)} F(a) \leq \sum_{a \leq c(K)} d_n(a)$$

where

$$c(K) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2(K)}\sqrt{D}$$

is the Minkowski constant of K, and it remains to recall the standard evaluation

$$\sum_{a\le x} d_n(a) = O(x\log^{n-1} x),$$

which can be easily proved by recurrence. □

For further reference we point out a special case:

Corollary. *If K is an imaginary quadratic field and $D = |d(K)|$, then*

$$h(K) \le \left(\frac{1}{\pi} + \frac{.35}{\log D}\right)\sqrt{D}\log D.$$

Proof : It suffices to note that

$$\sum_{a\le x} d_2(a) = \sum_{a\le x}\sum_{d|a} 1 = \sum_{d\le x}\left[\frac{x}{d}\right] \le x\sum_{a\le x}\frac{1}{a} \le x + x\log x,$$

and recall that in this case the Minkowski constant equals $2\sqrt{D}/\pi$. □

6. We conclude this section with the proof of the Pellet-Stickelberger theorem, concerning the quadratic character of polynomial and field discriminants.

Theorem 4.11. *If $f \in \mathbb{Z}[X]$ is monic and irreducible, and D denotes its discriminant, then for any odd prime $p \nmid D$ we have*

$$\left(\frac{D}{p}\right) = (-1)^{N-t},$$

where N is the degree of f and $t = t(p)$ denotes the number of irreducible factors of $\bar{f}$, the reduction of f mod p over the field $\mathbb{F}_p$.

Proof : Let $x_1, \dots, x_N$ be the roots of f, denote by L the splitting field of f over $\mathbb{Q}$ and by k the splitting field of $\bar{f}$ over $\mathbb{F}_p$. If $\mathfrak{P}$ is a prime ideal in R_L lying above $p\mathbb{Z}$, then $k_0 = R_L/\mathfrak{P}$ is a finite extension of $\mathbb{F}_p$, containing k. Let $s : R_L \longrightarrow k_0$ be the canonical map, and put $\bar{x}_i = s(x_i)$ $(i = 1, 2, \dots, N)$, so that $\bar{f}(X) = \prod_{i=1}^{N}(X - \bar{x}_i)$. Now put $\bar{D} = s(D)$ and note that $\bar{D} = \prod_{i<j}(\bar{x}_i - \bar{x}_j)^2$.

Observe that the elements $\bar{x}_i$ are distinct. Indeed, if $\bar{x}_r = \bar{x}_s$, then $x_r - x_s \in \mathfrak{P}$, and since $D = \prod_{i<j}(x_i - x_j)^2$, we get $D \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, thus $p|D$, contradiction. Therefore we can write $\bar{f} = F_1 \cdots F_t$, where the polynomials

$F_i \in \mathbb{F}_p[X]$ are distinct and irreducible. If we denote by $A_i = \{u_1^{(i)}, \ldots, u_{N_i}^{(i)}\}$ (with $N_i = \deg F_i$) the set of all roots of F_i in k, then we can write

$$\bar{D} = \prod_{i=1}^{r} D_i \prod_{s>i} B_{i,s}^2,$$

where

$$D_i = \prod_{r<s} (u_r^{(i)} - u_s^{(i)})^2$$

is the discriminant of F_i and

$$B_{i,s} = \prod_{\substack{x \in A_i \\ y \in A_s}} (x - y).$$

Since $B_{i,s}$ is invariant under the action of the Galois group of $k/\mathbb{F}_p$, we have $B_{i,s} \in \mathbb{F}_p$, and with a certain non-zero $B \in \mathbb{F}_p$ we obtain

$$\prod_{i=1}^{N} \prod_{s>i} B_{i,s}^2 = B^2.$$

If for a certain i we have $2 \nmid N_i$, then D_i is a square in the splitting field k_i of F_i over $\mathbb{F}_p$, but since $k_i/\mathbb{F}_p$ is cyclic of odd degree, D_i must be a square already in $\mathbb{F}_p$, since otherwise the field $\mathbb{F}_p(\sqrt{D_i})$ would be a subfield of k_i of degree 2. This shows that

$$\left(\frac{D}{p}\right) = 1$$

holds if and only if the product $\prod D_i$, taken over i's with $2|N_i$ is a square in F_p.

To decide when this happens observe that D_i is a square in $\mathbb{F}_p$ precisely when the product

$$\prod_{r<s} (u_r^{(i)} - u_s^{(i)})$$

lies in $\mathbb{F}_p$, and this occurs if and only if this product is invariant under the Galois group G_i of $k_i/\mathbb{F}_p$. Since for $g \in G_i$ the ratio

$$\frac{\prod_{r<s} (g(u_r^{(i)}) - g(u_s^{(i)}))}{\prod_{r<s} (u_r^{(i)} - u_s^{(i)})}$$

equals 1 if and only if the permutation induced by g in the set A_i is even, we obtain that D_i is a square in $\mathbb{F}_p$ precisely when all elements of G_i are even permutations. Now observe that this cannot happen for even N_i. Indeed, the group G_i is cyclic of N_i elements and acts transitively on A_i, thus its generator is a cycle of even length, which is an odd permutation. Therefore $\left(\frac{D}{p}\right) = 1$ holds if and only if the number of even N_i's is even. Since

$$N = \sum_{i=1}^{r} N_i = r + \sum_{i=1}^{r} (N_i - 1) \equiv r + \sum_{\substack{i \\ 2 | N_i}} 1 \pmod 2,$$

we arrive at our assertion. □

The following corollary results immediately:

Corollary. *Let a be an algebraic integer of degree n, f its minimal polynomial and p an odd rational prime, not dividing the discriminant of f. If $K = \mathbb{Q}(a)$, then*

$$\left(\frac{d(K)}{p}\right) = (-1)^{n-t_p},$$

where t_p is the number of irreducible factors of the reduction of f mod p. □

4.2. Different and Discriminant

1. In this section we shall define the discriminant for a relative extension. This cannot be done in the same way as in Chap. 2 for extensions of $\mathbb{Q}$, since we used there the existence of integral bases, which is assured only if the ring of integers of the ground field is a PID. Even if it is, and we imitate the procedure used for absolute extensions, we find that the discriminants of various integral bases may differ by a square of a unit, which is not necessarily equal to 1. So we have to use another approach. Since we want to use our constructions also for completions of algebraic number fields, we shall not restrict ourselves to finite extensions of $\mathbb{Q}$, but proceed as in the preceding section, assuming the conditions (i), (ii) and (iii) stated there. Thus L/K will be an extension degree n of a field K of zero characteristic, R will be a Dedekind domain with quotient field K, and S will be the integral closure of R in L. We assume moreover that R and S satisfy the finite norm property, have finite class-numbers, and for any ideal I of R we have $N(IS) = N(I)^n$.

Let $A \subset L$ be a non-zero R-module. The set

$$A^* = \{x \in L : \ T_{L/K}(xA) \subset R\}$$

will be called the *codifferent of A over K*. It is an R-module, which may even be equal to zero module. This happens if A is sufficiently large, e.g. $A = L$. To obtain non-trivial properties of the codifferent we have to make some additional assumptions on A. The most obvious thing to do is to assume that A is an S-module, or a fractional ideal in L.

Proposition 4.12. *If I is a fractional ideal in L, then its codifferent I^* is also a fractional ideal, and we have $II^* = S^*$. Moreover, if I is an ideal in S, then $(I^*)^{-1}$ is also an ideal in S.*

Proof : If $x_1, x_2 \in I^*$ and $b_1, b_2 \in S$, then

$$T_{L/K}((b_1x_1 + b_2x_2)I) \subset T_{L/K}(x_1I) + T_{L/K}(x_2I) \subset R,$$

whence I^* is an S-module. Since with a certain $a \in S$ we have $aI \subset S$ and $a \in I^*$, we see that I^* is non-zero. To show that with some non-zero $q \in S$ we have $qI^* \subset S$ let $\omega_1, \ldots, \omega_n$ be a K-basis of L, contained in S, and let b a non-zero element of $I \cap R$ (it can be an element of the form $N_{L/K}(c)$ with non-zero $c \in I \cap S$). We shall prove that the element $q = b \det \left[T_{L/K}(\omega_i\omega_j)\right]$, which is non-zero (as L/K is separable) and lies in R is good for us. Take any $x = c_1\omega_1 + \cdots + c_n\omega_n \in I^*$ with $c_k \in K$, and observe that since all elements $b\omega_k$ lie in I hence $T_{L/K}(bx\omega_k) \in R$. But

$$T_{L/K}(bx\omega_k) = b\sum_{i=1}^{n} c_i T_{L/K}(\omega_i\omega_k),$$

whence by Cramer's rule we infer that all elements $c_k b \det \left[T_{L/K}(\omega_i\omega_j)\right]$ lie in R, and so $qx \in S$, implying $qI^* \subset S$, as required.

The equality $II^* = S^*$ results now from the following chain of equivalences:

$$a \in I^* \Leftrightarrow T_{L/K}(aI) \subset R \Leftrightarrow T_{L/K}(aIS) \subset R \Leftrightarrow aI \subset S^* \Leftrightarrow a \in I^{-1}S^*.$$

To prove the final assertion observe that $I \subset S$ implies $S \subset I^*$, whence $(I^*)^{-1} = S(I^*)^{-1} \subset I^*(I^*)^{-1} = S$. □

If I is a fractional ideal in L, then $(I^*)^{-1}$, which is a fractional ideal by the last proposition (and in case $I \subset S$ even an integral ideal) will be called the *different* of I over K. We shall denote it by $D_{L/K}(I)$. The different of the unit ideal S will be called the *different of the extension* L/K and will be denoted by $D_{L/K}$.

Note that this notion depends not only on the extension L/K, but also on the choice of R. However, in all cases which we shall consider the choice of R will be obvious, so that no ambiguity will arise. Note also that the map $G(L) \to G(L)$ given by $I \mapsto D_{L/K}(I)$ is in general not a homomorphism.

We prove now some properties of the different.

Proposition 4.13. *(i) If $I \in G(L)$, then $D_{L/K}(I) = ID_{L/K}$.*

(ii) If $K \subset L \subset M$, then $D_{M/K}$ equals the product $D_{M/L}D_{L/K}$.

(iii) If L/K is normal, then $D_{L/K}$ is an ideal invariant under the action of the Galois group of L/K.

(iv) If $I \in G(K)$, then the conditions $T_{L/K}(J) \subset I$ and $J \subset ID_{L/K}^{-1}$ are equivalent for every $J \in G(L)$.

Proof : (i) By Proposition 4.12 we have

$$(D_{L/K}(I))^{-1} I D_{L/K} = I^* I D_{L/K} = S^* D_{L/K} = S,$$

and (i) results.

(ii) If W denotes the integral closure of R in M, then

$$T_{M/K}(D_{M/L}^{-1}(D_{L/K}^{-1}W)) = T_{L/K}(T_{M/L}(D_{M/L}^{-1}(D_{L/K}^{-1}W)))$$
$$= T_{L/K}(D_{L/K}^{-1} T_{M/L}(D_{M/L}^{-1})) \subset T_{L/K}(D_{L/K}^{-1} S) \subset R,$$

implying

$$D_{M/L}^{-1} D_{L/K}^{-1} \subset D_{M/K}^{-1},$$

and

$$D_{M/K} \subset D_{M/L} D_{L/K}.$$

On the other hand we have

$$T_{L/K}(T_{M/L}(D_{M/K}^{-1}W)) = T_{M/K}(D_{M/K}^{-1}W) \subset R,$$

thus $T_{M/L}(D_{M/K}^{-1}W) \subset D_{L/K}^{-1}$, and therefore

$$T_{M/L}(D_{L/K} D_{M/K}^{-1} W) = D_{L/K} T_{M/L}(D_{M/K}^{-1}W) \subset S,$$

implying

$$D_{L/K} D_{M/K}^{-1} \subset D_{M/L}^{-1},$$

and this gives

$$D_{M/K} \supset D_{L/K} D_{M/L},$$

hence (ii) results.

(iii) If $s \in Gal(L/K)$, then for $x \in S^*$ we have

$$T_{L/K}(s(x)S) = T_{L/K}(xs^{-1}(S)) = T_{L/K}(xS) \subset R,$$

hence $s(S^*) \subset S^*$, and also $s^{-1}(S^*) \subset S^*$, i.e., $S^* \subset s(S^*)$. Finally we get $s(S^*) = S^*$, and $s(D_{L/K}) = D_{L/K}$ follows.

(iv) It is enough to consider the sequence of equivalences

$$T_{L/K}(J) \subset I \Leftrightarrow I^{-1} T_{L/K}(J) \subset R$$
$$\Leftrightarrow I^{-1} J \subset D_{L/K}^{-1} \Leftrightarrow J \subset I D_{L/K}^{-1}. \qquad \square$$

Corollary 1. *$D_{L/K}^{-1}$ is the largest fractional ideal of L, all elements of which have their traces in R.*

Proof : Apply (iv) with $I = R$. $\square$

Now we can characterize extensions in which the trace map from S to R is surjective, and, more generally, identify the set $T_{L/K}(S)$.

Corollary 2. *The largest divisor of the ideal $D_{L/K}$ which lies in $i_{L/K}(I(R))$ equals $T_{L/K}(S)S$, and so $T_{L/K}(S)$ is the least common multiple of integral ideals $I \subset R$, satisfying $i_{L/K}(I)|D_{L/K}$.*

Proof : Since $T_{L/K}$ is an ideal in R it suffices to apply (iv) to $J = S$. □

Corollary 3. *The trace map $T_{L/K} : S \longrightarrow R$ is surjective if and only if the different $D_{L/K}$ does not have any divisor $\neq S$ lying in $i_{L/K}(I(R))$.*

Proof : Immediate by the preceding corollary. □

In the number-theoretic case one can prove more about the different and the codifferent.

Proposition 4.14. *If L is a finite extension of the rationals, $I \in G(L)$ has a $\mathbb{Z}$-basis $a_1, \ldots, a_n$, and $b_1, \ldots, b_n \in L$ satisfy*

$$T_{L/\mathbb{Q}}(a_i b_j) = \delta_i^j \quad (i, j = 1, 2, \ldots, n),$$

then the codifferent I^* is generated by the b_i's as a $\mathbb{Z}$-module. Moreover one has

$$N(D_{L/\mathbb{Q}}(I)) = N(I)|d(L)|,$$

and, in particular,

$$N(D_{L/\mathbb{Q}}) = |d(L)|.$$

Proof : Cramer's formulas imply that the b_i's are determined uniquely by the a_i's, and one sees easily, that they form a basis of the linear $\mathbb{Q}$-space L. For $x \in L$ and $y \in I$ write $x = \sum_{i=1}^n x_i b_i$, $y = \sum_{i=1}^n y_i a_i$ with $x_i \in \mathbb{Q}$ and $y_i \in \mathbb{Z}$. Then

$$T_{L/\mathbb{Q}}(xy) = \sum_{i,j} x_i y_j T_{L/\mathbb{Q}}(b_i a_j) = \sum_{i=1}^n x_i y_i,$$

and the last sum will lie in $\mathbb{Z}$ for every choice of $y \in I$ if and only if all x_i's are integral. This shows that $I^* = \bigoplus_{i=1}^n b_i \mathbb{Z}$.

(The same argument is also applicable in the more general situation, when R is a PID.)

To prove the second assertion it suffices, in view of Proposition 4.13 (i), to consider the case $I = R_L$. Let $\omega_1, \ldots, \omega_n$ be a integral basis of L. By the already proved part of the proposition the ideal $D_{L/\mathbb{Q}}^{-1}$ has a $\mathbb{Z}$-basis $b_1, \ldots, b_n$ such that

$$T_{L/\mathbb{Q}}(\omega_i b_j) = \delta_i^j.$$

Choose a natural m to make all numbers $c_i = mb_i$ integral, and consider the ideal $I = mD_{L/\mathbb{Q}}^{-1} \subset R_L$. Using Proposition 2.13 and its corollary we obtain

$$N(D_{L/\mathbb{Q}}^{-1})^2 = N(I)^2 N_{L/\mathbb{Q}}^{-2}(m) = \frac{d_{L/\mathbb{Q}}(c_1, \ldots, c_n)}{d(L)m^{2n}}$$
$$= \frac{d_{L/\mathbb{Q}}(b_1, \ldots, b_n)}{d(L)}.$$

Finally observe that the product $\left[\omega_i^{(j)}\right]\left[b_i^{(j)}\right]^T$ equals $\left[T_{L/\mathbb{Q}}(\omega_i b_j)\right]$, thus it coincides with the unit matrix and this leads to

$$d_{L/\mathbb{Q}}(b_1, \ldots, b_n) = d_{L/\mathbb{Q}}^{-1}(\omega_1, \ldots, \omega_n) = d(L)^{-1},$$

which gives $N(D_{L/\mathbb{Q}})^2 = d^2(L)$. □

2. Now we define the discriminant of the extension L/K. In contrast to the absolute discriminant it will not be an element of the ring R_K, but an ideal in this ring, however in the case $K = \mathbb{Q}$ it will coincide with the ideal generated by $d(L)$ in $\mathbb{Z}$. A definition of a discriminant which resembles more the absolute discriminant will be given in Chap. 6 in terms of ideles.

Our definition is very simple: the *discriminant* $d(L/K)$ of the extension L/K equals $N_{L/K}(D_{L/K})$. Proposition 4.14 immediately implies that $d(L/\mathbb{Q})$ is the ideal generated by $d(L)$.

Proposition 4.15. *If $K \subset L \subset M$, then*

$$d(M/K) = d(L/K)^{[M:L]} N_{L/K}(d(M/L)).$$

Proof : Follows from Proposition 4.13 (ii). □

Corollary 1. *If $Q \subset K \subset L$, then the discriminant $d(L)$ is divisible by $d(K)^{[L:K]}$.* □

This improves Proposition 2.16.

Corollary 2. *If $K/\mathbb{Q}$ is an extension with a square-free discriminant, then there is no field between $\mathbb{Q}$ and K.*

Proof : If L were such field, then by Corollary 2 to Theorem 2.22 there would be a prime divisor p od $d(L)$, and the preceding corollary would give $p^{[K:L]} | d(K)$. Therefore $d(L) = 1$, and Corollary 2 to Theorem 22 implies $L = \mathbb{Q}$. □

For an element $a \in S$, generating the extension L/K consider its minimal monic polynomial F, and define the *different* $\delta_{L/K}(a)$ of a as the value of the derivative F' at a. For convenience we define also the different for those elements of S which do not generate L/K, putting $\delta_{L/K}(a) = 0$ in that case.

Theorem 4.16. *The different $D_{L/K}$ is generated, as an ideal of S, by the set of all differents $\delta_{L/K}(a)$, with a running over S.*

Proof : For the proof we need some results concerning subrings of S having the form $A = R[a]$, i.e. generated by R and an element a of S such that $L = K(a)$. Obviously we have

$$R[a] = \bigoplus_{j=0}^{n-1} a^j R,$$

where $n = [L : K]$. For such rings it is possible to give an explicit set of generators for the codifferent, treated as an R-module:

Proposition 4.17. *If $a \in S$ generates the extension L/K, $A = R[a]$, $n = [L : K]$ and f is the minimal polynomial of a over R, then the codifferent A^* is generated as an R-module by the set $1/f'(a), a/f'(a), \ldots, a^{n-1}/f'(a)$, i.e.*

$$R[a]^* = \frac{1}{f'(a)} R[a].$$

Proof : Let B be the R-module generated by the set $\{a^j/f'(a)\}$ $(j = 0, 1, \ldots, n-1)$, and observe that if $a_1 = a, a_2, \ldots, a_n$ are the conjugates of a, then

$$\sum_{j=1}^{n} \frac{a_j^{k+1}}{f'(a_j)} \cdot \frac{f(X)}{X - a_j} = \begin{cases} X^{1+k}, & \text{if } 0 \leq k \leq n-2 \\ X^n - f(X) & \text{if } k = n-1. \end{cases}$$

Indeed, it suffices to note that on both sides we have polynomials of degrees $\leq n-1$, attaining the same values at n distinct points a_i. Putting $X = 0$ we obtain $T_{L/K}(a^k/f'(a)) \in R$, whence $a^k/f'(a) \in A^*$, i.e. $B \subset A^*$.

To obtain the converse inclusion let $b \in A^*$, and write $f(X) = c_n X^n + \cdots + c_0$, with $c_n = 1$. If we put

$$P(X) = \sum_{i=1}^{n} b_i \frac{f(X)}{X - a_i},$$

where $b_1 = b, b_2, \ldots, b_n$ are conjugates of b, then

$$P(X) = \sum_{j=1}^{n} c_j \sum_{k=0}^{j-1} X^k T_{L/K}(ba^{j-k-1}).$$

Since, by our choice of b, $T_{L/K}(bA) \subset R$, we see that the coefficients of P lie in R. But $bf'(a) = P(a) \in R[a]$, i.e. $b \in B$, thus $A^* \subset B$. □

Corollary. $f'(a)S \subset R[a]$.

Proof : $S \subset A^*$, hence $f'(a)S \subset f'(a)A^* = R[a]$. □

The greatest common divisor of ideals of S contained in A will be denoted by $\mathfrak{f}_A$ and called the *conductor* of A. The last proposition leads to a simple formula for it, and permits to obtain a relation between the different $D_{L/K}$ and the different $\delta_{L/K}(a)$ of an element $a \in S$, generating L/K.

Proposition 4.18. *Let a be an element of S, generating L/K, let f be its minimal polynomial over R, and let $A = R[a]$. Then*

(i) $\mathfrak{f}_A = \delta_{L/K}(a)D_{L/K}^{-1}$,

(ii) $\mathfrak{f}_A = \{x \in A : \ xS \subset A\}$,

(iii) $\mathfrak{f}_A = \{x \in L : \ xA^* \subset S^*\}$.

Proof : (i) Since $S^* \subset A^*$ the preceding proposition implies

$$\delta_{L/K}(a)D_{L/K}^{-1} = f'(a)S^* \subset R[a] \subset S,$$

thus the ideal $\delta_{L/K}(a)D_{L/K}^{-1}$ is integral and divisible by the conductor $\mathfrak{f}_A$. Moreover, from the proof of the last proposition we obtain that $T_{L/K}(A/f'(a))$ is contained in R. Therefore $T_{L/K}(\mathfrak{f}_A/f'(a)) \subset R$, hence $\mathfrak{f}_A/f'(a) \subset S^*$. Finally we get

$$\mathfrak{f}_A \subset f'(a)S^* \subset \delta_{L/K}(a)D_{L/K}^{-1}.$$

(ii) If $x \in \mathfrak{f}_A$, then

$$xS \subset \mathfrak{f}_A S = \mathfrak{f}_A \subset A,$$

showing that $\mathfrak{f}_A$ is contained in $\hat{A} = \{x \in A : \ xS \subset A\}$, and since $\hat{A}$ is an S-ideal contained in A, we get the converse inclusion $\hat{A} \subset \mathfrak{f}_A$.

(iii) Put $I = \{x \in L : \ xA^* \subset S^*\}$. For $x \in L$, $y \in S$ we have

$$yxA^* \subset yS^* \subset S^*,$$

and so I is a non-zero S-module. Moreover $IA^* \subset S^*$, which gives

$$T_{L/K}(IA^*) \subset T_{L/K}(S^*) \subset R,$$

hence $A^* \subset I^*$. Now (i) and Proposition 4.13 (i) imply now

$$A \subset f'(a)I^* = f'(a)I^{-1}D_{L/K}^{-1},$$

which in view of (i) leads to

$$I \subset IA \subset \delta_{L/K}(a)D_{L/K}^{-1} = \mathfrak{f}_A.$$

On the other hand, if $y \in A^*$, then

$$T_{L/K}(y\mathfrak{f}_A S) \subset T_{L/K}(yA) \subset R$$

hence $y\mathfrak{f}_A \subset S^*$ proving $\mathfrak{f}_A \subset I$. □

Corollary. *One has $S = R[a]$ if and only if the conductor of $A = R[a]$ equals S.*

Proof : If $\mathfrak{f}_A = S$, then $1 \in \mathfrak{f}$, and (ii) implies $S \subset A \subset S$. If $S = A$, then $1 \cdot S = S \subset A$, and by (i) we get $1 \in \mathfrak{f}_A$, i.e., $\mathfrak{f} = S$. □

For the proof of Theorem 4.16 we need two further lemmas.

Lemma 4.19. *Let $L = K(a)$ with $a \in S$, put $A = R[a]$, let $\mathfrak{P}$ be a prime ideal of S, and for $m = 1, 2, \ldots$ let $\phi_m : A/(A \cap \mathfrak{P}^m) \longrightarrow S/\mathfrak{P}^m$ be the homomorphism induced by the embedding $A \subset S$.*

(i) If $\mathfrak{P}$ does not divide the conductor $\mathfrak{f}_A$, then ϕ_m is an isomorphism, i.e., every residue class mod $\mathfrak{P}^m$ *in S can be represented by an element of A.*

(ii) Let $\mathfrak{p}$ be the prime ideal of R lying below $\mathfrak{P}$. Write $\mathfrak{p}S = \mathfrak{P}^e I$ with $\mathfrak{P} \nmid I$. If $a \in I \setminus \mathfrak{P}$ and the homomorphisms ϕ_m are isomorphisms for $m = 1, 2, \ldots$, then $\mathfrak{P} \nmid \mathfrak{f}_A$.

Proof : (i) Let $b \in \mathfrak{f}_A \setminus \mathfrak{P}$ and $c \in S$. Proposition 4.18 (ii) shows that for a certain $W \in R[X]$ we have $c = W(a)/b$. With a suitable $k > 0$ we have

$$b^k \equiv 1 \pmod{\mathfrak{P}^m},$$

and since $b = V(a)$ for some $V \in R[X]$, we obtain

$$c \equiv W(a)b^{k-1} \equiv W(a)V(a)^{k-1} \pmod{\mathfrak{P}^m},$$

thus every residue class mod $\mathfrak{P}^m$ is represented by an element from A.

(ii) Lemma 1.21 implies that every element of S may be written in the form $P(a)/D$ with $P \in R[X]$ and some fixed $D \in R$ (in fact, we can take $D = d_{L/K}(a)$). Let $\mathfrak{p}^m$ be the highest power of $\mathfrak{p}$ dividing D. Our assumption implies that every element $x \in S$ can be written in the form $x = b + y$ with $b \in A$ and $y \in \mathfrak{P}^{em}$. Then

$$ya^m \in \mathfrak{P}^{em} I^m = \mathfrak{p}^m S \subset D^{-1}\mathfrak{p}^m A.$$

Since $\mathfrak{p} \nmid D\mathfrak{p}^{-m}$ there exists $c \in D\mathfrak{p}^{-m} \setminus \mathfrak{p} \subset R$, and thus $ya^m \in c^{-1}A$, hence we can write $ya^m = c^{-1}r$ with $r \in A$. Then, with a suitable $V \in R[X]$ we get

$$y = \frac{r}{ca^m} = \frac{V(a)}{ca^m},$$

implying $ca^m x \in A$, whence $ca^m \in \mathfrak{f}_A$. However $ca^m \in A \setminus \mathfrak{P}$, and so $\mathfrak{P}$ does not divide $\mathfrak{f}_A$, as asserted. □

Lemma 4.20. *Let $\mathfrak{P}$ be a prime ideal of S, denote by $\mathfrak{p}$ the prime ideal of R lying below $\mathfrak{P}$, and let I be an ideal of S not divisible by $\mathfrak{P}$. Denote by k_0, k the fields $R/\mathfrak{p}$ and $S/\mathfrak{P}$, respectively, and let $y \in S \setminus \mathfrak{P}$ be such that $\bar{y} = y \bmod \mathfrak{P}$ generates the extension k/k_0. Let $F \in R[X]$ be such that $\bar{F}(X) \in k_0[X]$ is the minimal polynomial for $\bar{y}$, and assume that $F(y)$ does not lie in $\mathfrak{P}^2$. If now $a \in S$ generates the extension L/K and satisfies $a \in I$, $a \equiv y \,(\mathrm{mod}\ \mathfrak{P}^2)$, then for $m = 1, 2, \ldots$ every residue class $\bmod \mathfrak{P}^m$ in S can be represented by an element of $R[a]$.*

Proof : Let $x \in S$. Since $k = k_0[\bar{a}]$ there exists a polynomial $V \in R[X]$ such that $\bar{V}(\bar{a}) = x \bmod \mathfrak{P}$. Then obviously $x \equiv V(a) \,(\mathrm{mod}\ \mathfrak{P})$, proving our assertion in the case $m = 1$.

Assume now that our assertion holds for some $m \geq 1$ and let $x \in S$. Then for some $V \in R[X]$ we have $x \equiv V(a) \,(\mathrm{mod}\ \mathfrak{P}^m)$. The principal ideal generated by $F(a)$ in S is divisible by $\mathfrak{P}$, thus $F(a)S = \mathfrak{P}J$ with a certain ideal J, which is not divisible by $\mathfrak{P}$. Choose $u, u' \in S$ with $u \in J \setminus \mathfrak{P}$ and $uu' \equiv 1 \,(\mathrm{mod}\ \mathfrak{P})$. Moreover let $W \in R[X]$ be such that $u' \equiv W(a) \,(\mathrm{mod}\ \mathfrak{P})$. The element $c = (x - V(a))u^m / F^m(a)$ lies in S, thus there exists $T \in R[X]$ satisfying $c \equiv T(a) \,(\mathrm{mod}\ \mathfrak{P})$. Since $x = V(a) + cF^m(a)/u^m$, we obtain finally

$$x \equiv V(a) + T(a)F^m(a)W^m(a) \quad (\mathrm{mod}\ \mathfrak{P}^{m+1}). \qquad \square$$

Corollary. *For every prime ideal $\mathfrak{P}$ of S there exists $a \in S$ such that the conductor of the ring $R[a]$ is not divisible by $\mathfrak{P}$.*

Proof : Proposition 2.2 (ii) and Corollary 3 to Proposition 1.14 imply that there exist $a \in R$, satisfying the assumptions of the lemma. Lemma 4.19 (ii) shows now that the conductor of the ring $R[a]$ is not divisible by $\mathfrak{P}$. $\square$

To conclude the proof of our theorem observe that by Proposition 4.18 (i) every different $\delta_{L/K}(a)$ is contained in $D_{L/K}$, and $\mathfrak{f}_A D_{L/K} = \delta_{L/K}(a)S$ with $A = R[a]$ holds. Therefore it suffices to choose a as given by the Corollary to Lemma 4.20. $\square$

4. It has been observed by Weil [43] that the different $D_{L/K}$ is related to differentiations in commutative rings. If R is such a ring and M an R-module, then every homomorphism $f : R^+ \longrightarrow M^+$ of additive groups is called a *derivation*, provided it satisfies

$$f(uv) = uf(v) + vf(u) \tag{4.2}$$

for all $u, v \in R$.

Lemma 4.21. *Let $R \subset S$ and M be commutative rings and assume that M is at the same time an S-module. If $f : S \longrightarrow M$ is a derivation, vanishing at R, then for $a \in S$ and $P \in R[X]$ we have*

$$f(P(a)) = P'(a)f(a),$$

where P' is the formal derivative of P.

Proof : An easy induction gives $f(a^k) = ka^{k-1}f(a)$ for $k = 1, 2, \dots$, and it remains to recall that f is additive. □

In the case, when M is a commutative ring, a derivation f is called *essential*, if its image $f(R)$ contains at least one element which is not a zero-divisor. The connection between the existence of essential derivations and the different $D_{L/K}$ is given in the following theorem:

Theorem 4.22. *If I is an ideal of S, then an essential derivation $S \longrightarrow S/I$, vanishing on R exists if and only if I divides $D_{L/K}$.*

Proof : We need a lemma:

Lemma 4.23. *If $\mathfrak{P}$ is a prime ideal of S and $m \geq 1$, then for every derivation $f : S \longrightarrow S/\mathfrak{P}^m$ we have $f(\mathfrak{P}^{m+1}) = 0$.*

Proof : For $x \in \mathfrak{P}^{m+1}$ and $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ write $x = \pi^{m+1}A/B$ with $A \in S$, $B \in S \setminus \mathfrak{P}$, which is possible by Proposition 1.27 (i). Using Lemma 4.21 we get now

$$\begin{aligned} Bf(x) = Bf(x) + xf(B) = f(Bx) = f(\pi^{m+1}A) \\ = Af(\pi^{m+1}) = (m+1)A\pi^m f(\pi) = 0, \end{aligned}$$

and in view of $B \notin \mathfrak{P}$ we obtain $f(x) = 0$. □

Now observe that it suffices to establish the theorem for powers of prime ideals. Indeed, let $I = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. If $f : S \longrightarrow S/I$ is an essential derivation, equal to zero on R, then $f_i : S \longrightarrow S/\mathfrak{P}_i^{e_i}$ defined by $f_i(x) = f(x) \bmod \mathfrak{P}_i^{e_i}$ is also an essential derivation, vanishing at R. Conversely, if for $i = 1, 2, \dots, g$ we have essential derivations $f_i : S \longrightarrow S/\mathfrak{P}_i^{e_i}$, vanishing on R, then by putting $f(x) = \langle f_1(x), \dots, f_g(x) \rangle$ we obtain a derivation of S into the direct sum of the rings $S/\mathfrak{P}_i^{e_i}$, which is isomorphic with S/I, according to Theorem 1.15. Thus f can be regarded as a derivation of S into S/I, vanishing on R. To show that f is essential choose $x_1, \dots, x_g \in S$ so that $f_i(x_i)$ is not a zero divisor, and let $x \in S$ be a solution of the system $x \equiv x_i \pmod{\mathfrak{P}_i^{e_i+1}}$ $(i = 1, 2, \dots, g)$ of congruences. Such a solution exists by the Chinese remainder theorem, and since Lemma 4.23 implies $f_i(x) = f_i(x_i)$ for $i = 1, 2, \dots, g$ we see that $f(x)$ is not a zero-divisor.

Now assume that $f : S \longrightarrow S/\mathfrak{P}^m$ is an essential derivation vanishing on R, and choose $a \in S$ in such a way that for $A = R[a]$ we have $\mathfrak{P} \nmid \mathfrak{f}_A$, which

is possible by Corollary to Lemma 4.20. If $x \in S$ and $x \equiv W(a) \pmod{\mathfrak{P}^{m+1}}$ with $W \in R[X]$, then by Lemmas 4.21 and 4.23 we obtain

$$f(x) = f(W(a)) = W'(a)f(a).$$

Were $f(a)$ a divisor of zero, then $f(x)$ would be a zero-divisor for all $x \in S$, contrary to the assumption. Thus $f(a)$ is not a zero-divisor, and if we denote by $F \in R[X]$ the minimal polynomial of a over R, then

$$0 = f(0) = f(F(a)) = F'(a)f(a),$$

leading to $F'(a) \equiv 0 \pmod{\mathfrak{P}^m}$, and thus, by Proposition 4.18 (i), $\mathfrak{P}^m$ divides $D_{L/K}$, since $\mathfrak{P} \nmid \mathfrak{f}_A$.

Now assume that $\mathfrak{P}^m | D_{L/K}$, and use again Corollary to Lemma 4.20 to choose $a \in S$ so that the conductor $\mathfrak{f}_A$ of the ring $R[a]$ is not divisible by $\mathfrak{P}$. Moreover, let $b \in \mathfrak{f}_A \setminus \mathfrak{P}$, write $b = W(a)$ with $W \in R[X]$, and let $c \in S$ satisfy $bc \equiv 1 \pmod{\mathfrak{P}^m}$. Every element $x \in S$ can be written in the form $x = V(a)/b$ with a certain $V \in R[X]$, and we put now

$$f(x) = (V'(a)W(a) - V(a)W'(a))c^2 \pmod{\mathfrak{P}^m},$$

this definition being prompted by the familiar rule of differentiation of ratios. To check that this definition makes sense assume that we have $x = V_1(a)/b = V_2(a)/b$ with $V_1, V_2 \in R[X]$. Then $V_1(a) = V_2(a)$, hence we may write $V_1(X) - V_2(X) = F(X)G(X)$, where $F \in R[X]$ is the minimal polynomial of a and $G \in R[X]$. This implies

$$V_1'(a) - V_2'(a) = F'(a)G(a) \equiv 0 \pmod{\mathfrak{P}^m},$$

since by Theorem 4.16 $\mathfrak{P}^m \mid D_{L/K} \mid F'(a)S$.

It remains to check that f is an essential derivation. Since $f(u+v) = f(u) + f(v)$ clearly holds and $f(a) = 1$, it remains to check that (4.2) is satisfied. Let $u, v \in S$ and write $u = V_1(a)/b$, $v = V_2(a)/b$. Then

$$\begin{aligned} uf(v) + vf(u) &\equiv cV_1(a)\left(V_2'(a)W(a) - V_2(a)W'(a)\right)c^2 \\ &\quad + cV_2(a)\left(V_1'(a)W(a) - V_1(a)W'(a)\right)c^2 \\ &\equiv c^3\left(\left(V_1(a)V_2'(a) + V_1'(a)V_2(a)\right)W(a)\right. \\ &\quad \left. - 2V_1(a)V_2(a)W'(a)\right) \pmod{\mathfrak{P}^m}. \end{aligned}$$

Let $x = uv$ and write $x = P(a)/b$ with $P \in R[X]$. Since $V_1(a)V_2(a) = P(a)W(a)$, we may write $V_1(X)V_2(X) = P(X)W(X) + G(X)F(X)$ with $G \in R[X]$, and this leads to

$$V_1(a)V_2'(a) + V_1'(a)V_2(a) \equiv P'(a)W(a) + P(a)W'(a) \pmod{\mathfrak{P}^m},$$

and finally $uf(v) + vf(u) = f(x)$, as needed. □

Corollary. *The different $D_{L/K}$ equals the least common multiple of ideals I of S, for which there exists an essential derivation $f : S \longrightarrow S/I$ with $f(R) = 0$.* □

As an application of the theorem just obtained, we prove now one of the main results of the theory, the *different theorem.*

Theorem 4.24. *If $\mathfrak{P}$ is a prime ideal of S, $\mathfrak{p}$ is the prime ideal of R, lying below $\mathfrak{P}$, and $\mathfrak{p}S = \mathfrak{P}^e I$ with $\mathfrak{P} \nmid I$, then $\mathfrak{P}^{e-1} | D_{L/K}$. Moreover, if $(e, N(\mathfrak{P})) = 1$, then $\mathfrak{P}^e \nmid D_{L/K}$.*

Proof : The first part of the assertion can be obtained without the use of Theorem 4.22. Denote by M the least normal extension of K, containing L, let S_0 be the integral closure of R in M, and let $L_1, \ldots, L_n$ be the fields conjugated to L. Let $x \in \mathfrak{P}I$ and let p be the rational prime dividing $N(\mathfrak{P})$. For sufficiently large N we have

$$x^{p^N} \in (\mathfrak{P}I)^{p^N} \subset \mathfrak{p}S,$$

and, similarly, the elements $(x^{(i)})^{p^N}$ of the integral closure S_i of R in L_i, which are conjugated to x^{p^N}, lie in $\mathfrak{p}S_i$ for $i = 1, 2, \ldots, n$. This gives

$$T_{L/K}(x^{p^N}) \in \mathfrak{p}S_0 \cap R = \mathfrak{p}.$$

By the choice of p the difference $T_{L/K}(x^{p^N}) - T_{L/K}(x)^{p^N}$ lies in $\mathfrak{p}$, thus finally $T_{L/K}(x) \in \mathfrak{p}$. The resulting inclusion $T_{L/K}(\mathfrak{P}I) \subset \mathfrak{p}$ leads us, by Proposition 4.13 (i), to $\mathfrak{P}I \subset \mathfrak{p}D_{L/K}^{-1}$, $\mathfrak{P}ID_{L/K} \subset \mathfrak{p}S = \mathfrak{P}^e I$, and finally $D_{L/K} \subset \mathfrak{P}^{e-1}$, proving the first part of the theorem.

To prove the second part, assume that $(e, N(\mathfrak{P})) = 1$, i.e., e is not divisible by the characteristic of $R/\mathfrak{p}$. Let $f : S \longrightarrow S/\mathfrak{P}^e$ be a derivation, vanishing on R. In view of Theorem 4.22 it suffices now to show that every element of $f(S)$ is a zero-divisor. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ and $\Pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. With suitable $a, b \in S$, $a, b \notin \mathfrak{P}$ we have $\pi = \Pi^e a/b$, which gives

$$0 = \pi f(b) + bf(\pi) = f(\pi b) = f(\Pi^e a) = e\Pi^{e-1} f(\Pi)a,$$

showing that $f(\Pi)$ is a zero-divisor in $S/\mathfrak{P}^e$. Therefore $f(\Pi) \in \mathfrak{P}/\mathfrak{P}^e$. If now $x \in \mathfrak{P}^k$ with $k \geq 1$, then $x = \Pi^k a/b$ with $a, b \in S$, $b \notin \mathfrak{P}$, whence

$$bf(x) + xf(b) = k\Pi^{k-1} af(\Pi) + \Pi^k f(a) \in \mathfrak{P}/\mathfrak{P}^e.$$

and, in view of $xf(b) \in \mathfrak{P}/\mathfrak{P}^e$, we obtain $bf(x) \in \mathfrak{P}/\mathfrak{P}^e$. Since $b \notin \mathfrak{P}$ this shows that $f(x)$ is a zero-divisor. Finally, let $x \notin \mathfrak{P}$. By Theorem 1.18 we have $x^{N(\mathfrak{P})-1} = 1 + c$ with $c \in \mathfrak{P}$, and this gives

$$(N(\mathfrak{P}) - 1)x^{N(\mathfrak{P})-2} f(x) = f(x^{N(\mathfrak{P})-1}) = f(1 + c) = f(c).$$

Since $f(c)$ is a zero-divisor and $(N(\mathfrak{P})-1)x^{N(\mathfrak{P})-2} \notin \mathfrak{P}$, it follows that $f(x)$ is also a zero-divisor. □

Corollary 1. *The set of prime ideals of S ramified in L/K coincides with the set of all prime divisors of the different $D_{L/K}$.* □

Corollary 2. *There are only finitely many prime ideals ramified in a given extension L/K.* □

Corollary 3. *(The discriminant theorem) A prime ideal of R is ramified in the extension L/K if and only if it divides the discriminant $d(L/K)$.* □

Corollary 4. *There are no unramified extensions of degree > 1 of the rational field.*

Proof : Apply Corollary to Theorem 2.22 and the preceding corollary. □

Corollary 5. *If the extension L/K is tame, then the trace map $T_{L/K} : S \longrightarrow R$ is surjective.*

Proof : If the trace map is not surjective, then according to Corollary 3 to Proposition 4.13 there exists a proper ideal I of R such that IS divides the different $D_{L/K}$. Let $\mathfrak{P}$ be a prime ideal of S dividing IS, let $\mathfrak{p}$ be the prime ideal of R lying below $\mathfrak{P}$, denote by p the characteristic of the field $R/\mathfrak{p}$, and put $e = e_{L/K}(\mathfrak{P})$. Since we have $\mathfrak{p}|I$, and the tameness of L/K gives $p \nmid e$, hence

$$\mathfrak{P}^e|\mathfrak{p}S|IS|D_{L/K},$$

in contradiction to the theorem. □

It should be noted that there exist fields with unramified extensions. To give an example consider two square-free and relatively prime rational integers A, B, both congruent to unity mod 4 and distinct from 1, and put

$$K = \mathbb{Q}(\sqrt{AB}), \quad L = \mathbb{Q}(\sqrt{A}, \sqrt{B}).$$

Obviously we have $L = K(\sqrt{A}) = K(\sqrt{B})$. The differents of $\sqrt{A}$ and $\sqrt{B}$ over K are equal to $2\sqrt{A}$ and $2\sqrt{B}$, respectively, and so, by Theorem 4.16 we get $2 \in D_{L/K}$, because $(A, B) = 1$. Now choose $C, D \in \mathbb{Z}$ with $C^2 - 4D = A$. The root of the polynomial $X^2 + CX + D$ is an algebraic integer lying in L, and its different over K equals $\sqrt{A}$, showing that $A = (\sqrt{A})^2 \in D_{L/K}$. But $(A, 2) = 1$, and so the different $D_{L/K}$ contains two relatively prime rational integers, whence we get $D_{L/K} = R_L$, and Corollary 1 to the preceding theorem implies that the extension L/K is unramified. It follows from the class-field theory that every algebraic number field with class-number greater than 1 has an unramified extension with Abelian Galois group.

5. Now we shall consider the discriminant of a composite of two extensions of the same ground-field.

Proposition 4.25. *If the extension L/K is the composite of K_1/K and K_2/K, i.e., L is the minimal field containing K_1 and K_2 in a fixed algebraic closure of K, then the sets of prime ideals dividing $d(L/K)$ and $d(K_1/K)d(K_2/K)$ coincide.*

Proof : Proposition 4.15 shows that every prime ideal dividing the product $d(K_1/K)d(K_2/K)$ divides also $d(L/K)$. Assume now that $\mathfrak{p}$ is a prime ideal of R, dividing $d(L/K)$, but not dividing $d(K_1/K)$, and let $\mathfrak{P}$ be a prime ideal of S lying above $\mathfrak{p}$, and dividing $D_{L/K}$. If we would have $\mathfrak{P}|D_{K_1/K}S$, then, with $f = f_{L/K}(\mathfrak{P})$, we would get

$$\begin{aligned}\mathfrak{p}^f &= N_{L/K}(\mathfrak{P})|N_{L/K}(D_{K_1/K}S) = N_{K_1/K}(N_{L/K_1}(D_{K_1/K}S)) \\ &= N_{K_1/K}(D_{K_1/K}^{[L:K_1]}) = d(K_1/K)^{[L:K_1]},\end{aligned}$$

and thus $\mathfrak{p}|d(K_1/K)$, contrary to our assumption. Therefore $\mathfrak{P} \nmid D_{K_1/K}S$, and in view of $D_{L/K} = D_{L/K_1}D_{K_1/K}$ we get $\mathfrak{P}|D_{L/K_1}$. Now let $a \in K_2$ be integral over R with $K_2 = K(a)$, and denote by F, G its minimal polynomials over K and K_1, respectively. Then $L = K_1(a)$ and $F(X) = G(X)H(X)$ with $H \in K_1[X]$, thus $F'(a) = G'(a)H(a)$, and so $F'(a)$ lies in the ideal $G'(a)S$. By Theorem 4.16 we get $G'(a) \in D_{L/K_1} \subset \mathfrak{P}$, thus $F'(a) \in \mathfrak{P}$, and using again Theorem 4.16 we obtain $D_{K_2/K} \subset \mathfrak{P}$, showing that $\mathfrak{p}$ divides $d(K_2/K)$. □

Corollary 1. *(i) If $\mathfrak{p}$ is a prime ideal of R unramified in K_1/K and K_2/K, then it is also unramified in the composite extension K_1K_2/K.*

(ii) If the extensions K_1/K and K_2/K are both unramified, so is K_1K_2/K. □

Corollary 2. *If M/K is the minimal normal extension of K containing L, then the discriminants $d(L/K)$ and $d(M/K)$ have the same prime ideal divisors. In particular, if L/K is unramified, so is M/K.* □

In the case when the groundfield K equals $\mathbb{Q}$ we can in certain situations obtain more precise results.

Theorem 4.26. *Let for $i = 1, 2$ $K_i/\mathbb{Q}$ $(i = 1, 2)$ be a finite extension of degree n_i and discriminant $d(K_i)$, and assume $(d(K_1), d(K_2)) = 1$. Then the degree of the composite $L = K_1K_2$ equals n_1n_2, one has*

$$d(L) = d(K_1)^{n_2}d(K_2)^{n_1},$$

and if $\omega_1, \ldots, \omega_{n_1}$ is an integral basis of K_1 and $\Omega_1, \ldots, \Omega_{n_2}$ is an integral basis of K_2, then the set $\{\omega_i\Omega_j\}$ forms an integral basis of L.

Proof : Let K be the minimal normal extension of $\mathbb{Q}$ containing K_1. By Corollary 2 to Proposition 4.25 we have $(d(K), d(K_2)) = 1$. Let $K_1 = \mathbb{Q}(a)$, and let F, G be the minimal polynomials of a over $\mathbb{Q}$ and over K_2, respectively. Obviously G divides F, and to show that $F = G$ it suffices to prove that the coefficients of G are all rational. These coefficients lie in K, because they are rational functions of some conjugates of a over $\mathbb{Q}$, whence the field generated by them lies in $k = K \cap K_2$. By Proposition 2.16 we infer that $d(k)$ divides both $d(K)$ and $d(K_2)$ and hence equals ± 1. But according to Corollary 2 to Theorem 2.22 this can happen only if $k = \mathbb{Q}$, therefore $[K_1K_2 : K_2] = \deg G = \deg F = [K_1 : \mathbb{Q}]$, thus $F = G$, and the first assertion of the theorem follows.

To obtain the remaining parts observe that the discriminant of the system $\{\omega_i \Omega_j\}$ equals $\Delta = d(K_1)^{n_2} d(K_2)^{n_1}$, and so the discriminant of L is a divisor of Δ. Corollary 1 to Proposition 4.15 shows that $d(L)$ is divisible by $d(K_1)^{n_2}$ and by $d(K_2)^{n_1}$, and to conclude the proof one has only to note that these numbers are relatively prime, whence $d(L)$ has to be divisible by Δ, their product. □

Corollary. *Let for $i = 1, 2, \ldots, r$ $K_i/\mathbb{Q}$ be a finite extension of degree n_i, and let $\{\omega_j^{(i)}\}$ be its integral basis. If for $i \neq j$ we have $(d(K_i), d(K_j)) = 1$, then the discriminant of the composite extension $K = K_1K_2 \cdots K_r$ equals*

$$\prod_{i=1}^{r} d(K_i)^{n/n_i},$$

where $n = n_1 n_2 \cdots n_r$, and an integral basis is formed by the set $\{\prod_{i=1}^{r} \omega_{j_i}^{(i)}\}$.

Proof : Follows from the theorem by a simple inductive argument. □

6. The last theorem permits us now to give a description of principal properties of cyclotomic fields. Let $K_m = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field. Observe that for odd m the fields K_m and K_{2m} coincide, because $-\zeta_m$ generates K_{2m}, whence it suffices to deal in sequel only with the case when m is not congruent to 2 mod 4.

Theorem 4.27. *(i) For all $m, n \geq 1$ we have $K_mK_n = K_{[m,n]}$.*
(ii) For $m \geq 1$ we have $[K_m : \mathbb{Q}] = \varphi(m)$,

$$d(K_m) = \prod_{p^a \| m} d(K_{p^a})^{\varphi(m/p^a)},$$

and $1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ is the integral basis of K_m. Moreover the extension $K_m/\mathbb{Q}$ is normal with its Galois group isomorphic to $G(m)$, the multiplicative group of residue classes mod *m, prime to m, the isomorphism being given*

by $r \mapsto g_r$, *with* $g_r(\zeta_m) = \zeta_m^r$. *Finally, the minimal polynomial of* ζ_m *over* $\mathbb{Q}$ *equals*

$$F_m(X) = \prod_{\substack{1 \le j \le m \\ (j,m)=1}} (X - \zeta_m^j) = \frac{X^m - 1}{\left(X^m - 1, \prod_{j<m}(X^j - 1)\right)},$$

(iii) If $m \not\equiv 2 \pmod 4$, *then* $K_m \subset K_n$ *holds if and only if* $m|n$, *thus for distinct* m, n, *both incongruent to* $2 \bmod 4$ *the fields* K_m *and* K_n *are distinct.*

(iv) If $m|n$, *then the subgroup of* $G(n)$, *corresponding to* K_m *according to the Galois theory equals*

$$\{r \in G(n) : \ r \equiv 1 \pmod m\},$$

(v) For all m, n *we have* $K_m \cap K_n = K_{(m,n)}$.

(vi) If $m < n$ *and* $K_m = K_n$, *then* m *is odd and* $n = 2m$.

Proof : (i) If $[m, n] = s$, then

$$\zeta_m = \zeta_s^{s/m}, \quad \zeta_n = \zeta_s^{s/n},$$

thus $K_m K_n \subset K_s$. To get the converse inclusion, solve

$$mx + ny = (m, n) = \frac{mn}{s}$$

in rational integers x, y, and observe that

$$\zeta_m^y \zeta_n^x = \zeta_s,$$

thus $K_s \subset K_m K_n$.

(ii) If $m = \prod_p p^{\alpha_p}$ is the canonical factorization of m, then by (i) K_m is the composite of the fields $K_{p^{\alpha_p}}$, which by Theorem 2.20 have their discriminants relatively prime, so we may apply Corollary to Theorem 4.26 to obtain the formula for the discriminant and the statements about the degree and integral basis. The normality of the extension $K_m/\mathbb{Q}$ follows from the observation that all conjugates of ζ_m are powers of ζ_m, and since Proposition 2.16 and Corollary to Theorem 2.22 imply that the intersection of $K_{p^{\alpha_p}}$ and $K_{mp^{-\alpha_p}}$ equals $\mathbb{Q}$, it follows that $K_m/\mathbb{Q}$ has its Galois group isomorphic to $G(m)$. Moreover, if $(j, m) = 1$, then $\mathbb{Q}(\zeta_m^j) = K_m$, since $jr \equiv 1 \pmod m$ implies $(\zeta_m^j)^r = \zeta_m$. Because $[K_m : \mathbb{Q}] = \varphi(m)$, and every conjugate of ζ_m is an m-th primitive root of unity, we obtain that the set of conjugates of ζ_m coincides with $\{\zeta_m^j : \ (j, m) = 1\}$, This establishes the assertion about F_m. The statement concerning the isomorphism between the Galois group and $G(m)$ results now immediately.

(iii) If $m|n$, then $\zeta_m = \zeta_n^{n/m}$, implying $K_m \subset K_n$. Conversely, if $K_m \subset K_n$, then denoting by N the order of the group $E(K_n)$ we get with a suitable a the equality $\zeta_n = \zeta_N^a$, implying $n|N$. Obviously $K_n = K_N$ and so (ii) gives $\varphi(n) = \varphi(N)$. Because of $n|N$ this is possible if either $N = n$, or n is odd and

$N = 2n$. In both cases ζ_m is a power of ζ_N, so $m|N$ thus either $m|n$ or $m|2n$, in which case for m odd we get $m|n$, and if m is even, then $m \equiv 2 \pmod 4$, which is excluded by our assumption.

(iv) Let H be the subgroup of $G(n)$ corresponding to K_m. Clearly r lies in H if and only if $g_r(\zeta_m) = \zeta_m$. Now observe that with $q = n/m$ we have $\zeta_m = \zeta_n^q$ and $g_r(\zeta_m) = g_r(\zeta_n^q) = \zeta_n^{rq}$, showing that r belongs to H if and only if $rq \equiv q \pmod n$, which is equivalent to $r \equiv 1 \pmod m$.

(v) Let $d = (m, n)$ and $D = [m, n]$. By (i) the fields K_d, K_m and K_n are contained in K_D. If for $r|D$ we denote by H_r the subgroup of $G(D)$ corresponding to K_r, then (iv) implies that $K_m \cap K_n$ corresponds to the group $H_m H_n$, equal to

$$\{s \bmod D : \ s = r_1 r_2, r_1 \equiv 1 \pmod m, \ r_2 \equiv 1 \pmod n, (s, D) = 1\}.$$

We have to show that $H_m H_n = H_d$. The inclusion $H_m H_n \subset H_d$ being immediate, take $s \in H_d$ and solve the systems of congruences

$$x \equiv s \pmod m, \quad x \equiv 1 \pmod n,$$

and

$$y \equiv 1 \pmod m, \quad y \equiv s \pmod n,$$

which is possible in view of $s \equiv 1 \pmod d$. Now we get

$$x \bmod D \in H_n, \quad y \bmod D \in H_m \text{ and } xy \equiv s \bmod D,$$

proving $s \in H_m H_n$.

(vi) If $m < n$ and $K_m = K_n$, then (iii) implies that $n \equiv 2 \pmod 4$, since $n \nmid m$. Writing $n = 2q$ with odd q we get $K_m = K_q$. Applying again (iii) we get $q|m$, because $q \not\equiv 2 \pmod 4$. Now it suffices to observe that $q|m < n = 2q$, hence $q = m$, as asserted. □

Corollary. *One has*

$$\#E(K_m) = \begin{cases} m & \text{if } m \text{ is even,} \\ 2m & \text{if } m \text{ is odd.} \end{cases}$$

Proof : If $T = \#E(K_m)$, then $T \geq m$ and $K_T = K_m$. If $T > m$, then (vi) implies $T = 2m$ with odd m. □

The polynomial $F_m(X)$ occuring in the last theorem is called the m-th *cyclotomic polynomial*. We have seen above how its irreducibility over $\mathbb{Q}$ follows from the theory of fields, but there are several shorter direct proofs. We present here one, due to K.Grandjot [12], based on Dirichlet's prime number theorem and the fact that the binomial coefficients $\binom{p}{k}$ are for $k = 1, 2, \ldots, p-1$ divisible by p:

Let $V \in \mathbb{Z}[X]$ have ζ_m for one of its roots. It suffices to show that for every j prime to m the number ζ_m^j is also a root of V. For every prime p congruent to j mod m we have

$$0 \equiv V(\zeta_m)^p \equiv V(\zeta_m^p) \equiv V(\zeta_m^j) \pmod{pR_{K_m}},$$

and this shows that the algebraic integer $V(\zeta_m^j)$ is divisible by infinitely many prime ideals, hence it vanishes, as asserted. □

7. If the extension L/K is normal with Galois group G, then the question arises of determining the structure of L as a $K[G]$-module and of S as an $R[G]$-module, the group ring acting by

$$(\sum_{g \in G} a_g g)x = \sum_{g \in G} a_g g(x).$$

The structure of L as a $K[G]$-module is described by the following theorem of Noether:

Theorem 4.28. *If K is an infinite field, and L/K is its finite normal separable extension with Galois group G, then L is isomorphic to $K[G]$ as an $K[G]$-module.*

(For finite K this is also true, but the proof is different.)

Proof : We follow Waterhouse [79] and start with a result of Dedekind on linear independence of automorphisms:

Lemma 4.29. *If $g_1, \ldots, g_N$ are distinct automorphisms of a field L, and for certain $c_1, \ldots, c_N \in L$ one has*

$$c_1 g_1(x) + \cdots + c_N g_N(x) = 0 \tag{4.3}$$

for all $x \in L$, then $c_1 = \cdots = c_N = 0$.

Proof : Assume that the assertion is false, and select a sum

$$\sum_{j=1}^{N} c_j g_j(x)$$

with non-zero $c_j \in L$, which vanishes for all $x \in L$, and for which the number N of summands is minimal. Clearly $N \geq 2$. If we choose now $y \in L$ with $g_1(y) \neq g_2(y)$, then

$$0 = \sum_{i=1}^{N} c_i g_i(xy) = \sum_{i=1}^{N} c_i g_i(x) g_i(y),$$

and since obviously $g_1(y) \neq 0$, we get

$$\sum_{i=1}^{N} c_i g_i(x) g_i(y) g_1(y)^{-1} = 0.$$

Subtracting this equality from (4.3) we arrive at a vanishing linear combination of automorphisms with fewer non-zero terms, contradicting the choice of N. □

Now let $g_1 = e, g_2, \ldots, g_n$ be all the elements of G, and observe that the set of all vectors of the form

$$\langle g_1(x), g_2(x), \ldots, g_n(x) \rangle,$$

with $x \in L$, generates the linear space L^n, because the lemma shows that they cannot all lie in a proper subspace.

This shows that there exist elements $c_1, x_1, \ldots, c_n, x_n$ of L satisfying

$$\sum_{i=1}^{n} c_i x_i = 1 \quad \text{and} \quad \sum_{i=1}^{n} c_i g_j(x_i) = 0 \quad (j = 2, 3, \ldots, n).$$

The polynomial

$$P(X_1, \ldots, X_n) = \det \left[\sum_{i=1}^{n} X_i h^{-1} g(x_i) \right]_{g,h \in G}$$

does not vanish identically, since $P(c_1, c_2, \ldots, c_n) = 1$. Since K is infinite, there are elements $u_1, \ldots, u_n$ in K such that $P(u_1, \ldots, u_n) \neq 0$, and this gives, with $A = \sum_{i=1}^{n} u_i x_i$,

$$\det \left[h^{-1} g(A) \right]_{g,h \in G} = P(u_1, \ldots, u_n) \neq 0.$$

This implies that the set $\{g(A) : g \in G\}$ is K-linearly independent. Indeed, if we had $\sum_{g \in G} d_g g(A) = 0$, with $d_g \in K$, not all zero, then for every $h \in G$ we would obtain

$$\sum_{g \in G} d_g h^{-1} g(A) = 0,$$

and so $\det \left[h^{-1} g(A) \right]_{g,h \in G} = 0$, a contradiction.

Finally observe that the map $K[G] \longrightarrow L$, defined by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g(A)$$

is K-linear, preserves the action of G and is surjective, since its image contains n K-linearly independent elements and $\dim_K L = n$, whence it is an isomorphism of $K[G]$-modules. □

One can ask whether an analogous result is true for the ring S, i.e. whether S is isomorphic to $R[G]$ as an $R[G]$-module. The answer is negative in general, as the example $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ shows. If $K = \mathbb{Q}$ and the answer is positive, then one says that the extension $L/\mathbb{Q}$ has a *normal integral basis*.

We give now a simple necessary condition for $S \sim R[G]$:

Proposition 4.30. *If L/K is normal with Galois group G and $S \sim R[G]$, then the trace map $T_{L/K} : S \longrightarrow R$ is surjective.*

Proof : If $f : R[G] \longrightarrow S$ is an isomorphism of $R[G]$-modules and $a = f(e)$, e being the unit element of G, then for $x \in R$ we have with suitable $a_g \in R$ $(g \in G)$

$$x = f(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g f(ge) = \sum_{g \in G} a_g g(a),$$

thus for all $h \in G$

$$x = h(x) = \sum_{g \in G} a_g hg(a) = \sum_{g \in G} a_{h^{-1}g} g(a),$$

and we infer that the coefficients a_g are independent of g, whence

$$x = a_e \sum_{g \in G} g(a) = a_e T_{L/K}(a) = T_{L/K}(a_e a).$$

Thus the trace is surjective. □

Corollary 1. *If L/K is normal of degree n with Galois group G, and S is isomorphic to $R[G]$, then the discriminant $d(L/K)$ cannot be divisible by an n-th power of a prime ideal.*

Proof : Applying Corollary 3 to Proposition 4.13 we find that $D_{L/K}$ is not divisible by proper ideals of R. By Proposition 4.13 (iii) we obtain

$$d(L/K)S = N_{L/K}(D_{L/K})S = D_{L/K}^n,$$

thus if $\mathfrak{p}$ were a prime ideal of R with $\mathfrak{p}^n | d(L/K)$, then we would have $\mathfrak{p}^n S | D_{L/K}^n$ and $\mathfrak{p}S | D_{L/K}$, a contradiction. □

Corollary 2. *If $K/\mathbb{Q}$ is normal of degree n and has a normal integral basis, then $d(K)$ is not divisible by the n-th power of a prime.*

Proof : The assertion results from the preceding corollary and Proposition 4.14. □

We shall see later that if L/K is normal, then the trace map is surjective if and only if the extension L/K is tame (see Corollary 3 to Proposition 6.2).

The condition given in Corollary 2 above is in general not sufficient for the existence of a normal integral basis.

We prove now certain simple results, permitting us to obtain normal integral bases in some extensions of $\mathbb{Q}$.

Proposition 4.31. *(i) If $\mathbb{Q} \subset K \subset L$, both extensions $L/\mathbb{Q}$, $K/\mathbb{Q}$ are normal, and $L/\mathbb{Q}$ has a normal integral basis, then $K/\mathbb{Q}$ also has a normal integral basis. In fact, if an integral basis of $L/\mathbb{Q}$ is formed by conjugates of $a \in L$, then the conjugates of $T_{L/K}(a)$ form a normal integral basis of $K/\mathbb{Q}$.*

(ii) If the normal extensions $K_i/\mathbb{Q}$ $(i = 1, 2, \ldots, m)$ have normal integral bases, and their discriminants are pairwise relatively prime, then their composite $L = K_1 \cdots K_m$ has a normal integral basis.

Proof : (i) Let G be the Galois group of $L/\mathbb{Q}$, and let $\{g(a) : g \in G\}$ be a normal integral basis of L. Let H be the subgroup of G fixing K. An integer $x = \sum_{g \in G} A_g g(a)$ $(A_g \in \mathbb{Z})$ lies in R_K if and only if for all $h \in H$ we have $h(x) = x$, and since

$$h(x) = \sum_{g \in G} A_{h^{-1}g} g(a),$$

this occurs precisely when for all $h \in H$ we have $A_{hg} = A_g$. It follows that if $X_1 = H, X_2, \ldots, X_m$ are cosets mod H in G, then every $x \in R_K$ can be uniquely written in the form $x = \sum_{i=1}^{m} A_i \omega_i$ with $\omega_i = \sum_{g \in X_i} g(a)$ with $A_i \in \mathbb{Z}$. This shows that $\omega_1, \ldots, \omega_m$ is an integral basis of K. Since the ω_i's are all conjugated to $\omega_1 = T_{L/K}(a)$, the assertion (i) follows.

(ii) This follows from the observation that the integral basis of L, constructed from the normal integral bases of the fields K_i with the use of Corollary to Theorem 4.26 is invariant under the action of the Galois group of L. □

Corollary. *The m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ has a normal basis if and only if m is square-free.*

Proof : Theorem 2.20 shows that if $m = p$ is a prime, then the set

$$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$$

is a normal integral basis, hence the existence of a normal integral basis in K_m for m square-free results from part (ii) of the proposition.

If m is not square-free, then for a certain prime p we have $p^2 | m$, implying $L = K_{p^2} \subset K_m$, and in view of part (i) of the proposition it remains to show that L does not have a normal integral basis. Now Theorem 2.20 gives $[L : Q] = p^2 - p$ and $|d(L)| = p^c$ with $c = 2p^2 - 3p$, and since $2p^2 - 3p \geq p^2 - p$, Corollary 2 to Proposition 4.30 shows that L does not have a normal integral basis. □

We shall prove in Chap. 6 (Theorem 6.18) that every Abelian extension of the rationals is a subfield of a suitable cyclotomic field, and from this result a criterion for the existence of a normal integral basis in Abelian fields will follow.

4.3. Factorization of Prime Ideals in Extensions. More about the Class-group

1. We shall now consider the question of establishing effectively the decomposition of a prime ideal $\mathfrak{p}$ of R into prime ideals of S. In many cases this can be done with the use of Theorem 4.33 below, whose certain special cases go back to Kummer, and which was proved by Dedekind for rings of algebraic integers. We need first an analogue of Lemma 4.20:

Lemma 4.32. *Let $\mathfrak{p}$ be a prime ideal of R, a an element of S, generating the extension L/K and $n = [L : K]$. Further let $A = R[a]$ and let $\mathfrak{f}$ be the conductor of A. Then the following conditions are equivalent:*

(i) $\mathfrak{p}S \cap A = \mathfrak{p}[a]$,

(ii) The embedding of A in S induces an isomorphism $f : A/(A \cap \mathfrak{p}S) \longrightarrow S/\mathfrak{p}S$, i.e., every coset of S mod $\mathfrak{p}S$ contains an element of A,

(iii) The embedding of A in S induces an isomorphism $A/(A \cap \mathfrak{p}^m S) \longrightarrow S/\mathfrak{p}^m S$, i.e., every coset of S mod $\mathfrak{p}^m S$ contains an element of A for $m = 1, 2, \ldots$.

(iv) For $m = 1, 2, \ldots$ we have $A \cap \mathfrak{p}^m S = \mathfrak{p}^m[a]$,

(v) $\mathfrak{p} \nmid N_{L/K}(\mathfrak{f})$,

(vi) The rational prime p, lying in $\mathfrak{p}$ does not divide the index $[S : R[a]]$.

Proof : (i) $\Rightarrow$ (ii). Since $\#(S/\mathfrak{p}S) = N(\mathfrak{p}S) = (N\mathfrak{p})^n$ and $\#(A/(A \cap \mathfrak{p}S)) = \#(A/\mathfrak{p}[a]) = N(\mathfrak{p})^n$, the homomorphism f is surjective, and since it is obviously injective, we obtain (ii).

(ii) $\Rightarrow$ (iii). For $m = 1$ the assertion is true by assumption. Assume now that (iii) holds for a certain $m \geq 1$, and choose $c \in \mathfrak{p} \setminus \mathfrak{p}^2$, write $cR = \mathfrak{p}I$ (with $\mathfrak{p} \nmid I$), choose $d \in I \setminus \mathfrak{p}$, let $d' \in R$ satisfy $dd' \equiv 1 \pmod{\mathfrak{p}^m}$, and finally let b be an arbitrary element of S. By assumption there exists a polynomial $V \in R[X]$ such that $b \equiv V(a) \pmod{\mathfrak{p}^m S}$, and therefore $b_1 = (b - V(a))d^m c^{-m}$ lies in S. If we now choose $W \in R[X]$ so that $b_1 \equiv W(a) \pmod{\mathfrak{p}S}$, then we arrive at

$$b = V(a) + b_1 c^m d^{-m} \equiv V(a) + (cd')^m W(a) \pmod{\mathfrak{p}^{m+1} S},$$

whence (iii) holds for $m + 1$.

(iii) $\Rightarrow$ (iv). It suffices to note that $\mathfrak{p}^m[a]$ is contained in $A \cap \mathfrak{p}^m S$ and the indices of both these rings are equal to $N(\mathfrak{p})^{mn}$ by (iii).

(iv) $\Rightarrow$ (i). This implication is obvious.

(iii) $\Rightarrow$ (v). Let $F \in R[X]$ be the minimal polynomial of a, write

$$N_{L/K}(F'(a))R = \mathfrak{p}^m I$$

with $\mathfrak{p} \nmid I$, choose $b \in I \setminus \mathfrak{p}$, and let $c \in S$. By (iii) there exists $d \in A$ such that $b(c-d)/N_{L/K}(F'(a))$ lies in S, therefore $b(c-d)/F'(a) \in S$ and we obtain $b(c-d) \in F'(a)S \subset A$ by Corollary to Proposition 4.17. Since $b \in R$ and $d \in A$, we get $bd \in A$, and finally $bc \in A$. As $c \in S$ was arbitrary, this implies $b \in \mathfrak{f}$. It remains to observe that $N_{L/K}(b) = b^n \notin \mathfrak{p}$ and $N_{L/K}(b) \in N_{L/K}(\mathfrak{f})$, hence $\mathfrak{p} \nmid N_{L/K}(\mathfrak{f})$.

(v) $\Rightarrow$ (ii). If $\mathfrak{p} \nmid N_{L/K}(\mathfrak{f})$ and $\mathfrak{p}S = \prod_i \mathfrak{P}_i^{e_i}$, then none of the $\mathfrak{P}_i$'s divides $\mathfrak{f}$. Corollary 3 to Proposition 1.14 gives the existence of $b \in \mathfrak{f}$, with $b-1 \in \mathfrak{P}_i$ for all $\mathfrak{P}_i$'s dividing $\mathfrak{p}$. Then $b \in \mathfrak{f} \subset A$, hence we may write $b = V(a)$ with a certain $V \in R[X]$, and therefore every $c \in S$ may be put in the form $c = W(a)/b = W(a)/V(a)$ for suitable $W \in R[X]$. Since $(bS, \mathfrak{p}S) = 1$, we have for a suitable $r > 0$ the congruence $V(a)^r \equiv 1 \pmod{\mathfrak{p}S}$, whence

$$c \equiv W(a)V(a)^{r-1} \pmod{\mathfrak{p}S}.$$

We have proved the equivalence of the conditions (i) - (v), and it remains to prove that the last condition is also equivalent to them.

(vi) $\Rightarrow$ (v). Write $m = [S : R[a]]$, and note that if $b \in S$, then $mb \in A$, therefore $m \in \mathfrak{f}$, and thus $\mathfrak{f}$ divides the ideal mS. Taking norms we get $N_{L/K}(\mathfrak{f}) | N_{L/K}(mS) = m^n S$, showing that every prime ideal of R dividing $N_{L/K}(\mathfrak{f})$ must also divide mR.

(ii) & (iv) $\Rightarrow$ (vi). Again put $m = [S : R[a]]$, and assume that the rational prime p lying in $\mathfrak{p}$ divides m. Then there exists $c \in S \setminus A$ with $pc \in A$. It follows from (ii) that there are polynomials $V, W \in R[X]$ of degrees $\leq n-1$, such that $pc = V(a)$, and $c = W(a) + b$ with $b \in \mathfrak{p}S$. Since $c \notin A$, we have $V \notin pR[X]$. Let $pR = \prod_i \mathfrak{p}_i^{e_i}$ be the factorization of pR in R, and observe that $V(a) - pW(a) = pb$, hence

$$V(a) \in pS \cap A \subset \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} S \cap A \subset \mathfrak{p}_j^{e_j},$$

for $j = 1, 2, \ldots, g$. Now we use (iv) to obtain $V(a) \in \mathfrak{p}_j^{e_j}[a]$, so all coefficients of the polynomial $V(X)$ lie in $\mathfrak{p}_j^{e_j}$ for $j = 1, 2, \ldots, g$. But this implies that all coefficients of V lie in pR, and therefore $c \in A$, contradiction. □

We may state now the main result of this section:

Theorem 4.33. *Let $a \in S$ be a generating element for the extension L/K, and let $f \in R[X]$ be its minimal polynomial. Moreover let $\mathfrak{p}$ be a prime ideal of R satisfying the equivalent conditions of Lemma 4.32, and denote by k the field $R/\mathfrak{p}$. Let φ be the map $R[X] \longrightarrow R[X]/\mathfrak{p}[X] = k[X]$ resulting from the application of the canonical map $R \longrightarrow k$ to every coefficient. If*

$$\varphi(f) = f_1^{e_1} \cdots f_g^{e_g},$$

where the f_i's are distinct monic and irreducible polynomials over k, then

$$\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$ are distinct prime ideals of S, $f_{L/K}(\mathfrak{P}_i) = \deg f_i$, and

$$\mathfrak{P}_i = \mathfrak{p}S + F_i(a)S \quad (i = 1, 2, \ldots, g),$$

where $F_i \in R[X]$ is any polynomial satisfying $\varphi(F_i) = f_i$.

Proof : Consider the residue maps

$$\varphi_i : \ k[X] \longrightarrow k[X]/f_i k[X] = k_i$$

for $i = 1, 2, \ldots, g$, and denote by Φ_i the composition $\varphi_i \circ \varphi : R[X] \longrightarrow k_i$. Observe that the kernel of Φ_i equals $I_i = \mathfrak{p}[X] + F_i(X)R[X]$ of $R[X]$. In fact, I_i is evidently contained in Ker Φ_i, and if $V \in$ Ker Φ_i, then $\varphi(V) \in$ Ker φ_i, whence for a suitable $h \in k[X]$ we have $\varphi(V) = h(X)f_i(X)$, i.e. $V(X) = A(X) + B(X)F_i(X)$ with certain $A \in \mathfrak{p}[X]$ and $B \in R[X]$. Thus $V \in I_i$.

The principal ideal generated by f in $R[X]$ is divisible by I_i, hence the homomorphism Φ_i induces a map of $R[X]/fR[X]$ into k_i. But $R[X]/fR[X]$ is isomorphic to $R[a]$, and so, using this isomorphism, we obtain a map

$$\psi_i : \ R[a] \longrightarrow k_i,$$

which is easily seen to be surjective. Its kernel consists of elements $V(a)$ with $V \in I_i$, hence equals $\mathfrak{p}[a] + F_i(a)R[a]$.

After these preparations we define now a map of S into k_i in the following way:

Let $b \in S$, choose, using Lemma 4.32 (ii), a polynomial $V \in R[X]$ with $b \equiv V(a) \pmod{\mathfrak{p}S}$, and define

$$\Psi_i(b) = \psi_i(V(a)).$$

The map Ψ_i is well defined, since if $V(a) \equiv 0 \pmod{\mathfrak{p}S}$, then Lemma 4.32 (i) implies $V(a) \in \mathfrak{p}S \cap A = \mathfrak{p}[a]$, and so $\psi_i(V(a)) = 0$.

The map Ψ_i is surjective, because ψ_i was such. This shows that the ideal $\mathfrak{P}_i =$ Ker Ψ_i is a non-zero prime ideal in S. Now note that $\mathfrak{P}_i = \mathfrak{p}S + F_i(a)S$. In fact, we have

$$\begin{aligned}\mathfrak{P}_i &= \{c \in S : \ c \equiv V(a) \pmod{\mathfrak{p}S}, V \in R[X], V[a] \in \mathfrak{p}[a] + F_i(a)A\} \\ &= \mathfrak{p}S + \mathfrak{p}[a] + F_i(a)A = \mathfrak{p}S + F_i(a)A = \mathfrak{p}S + F_i(a)S,\end{aligned}$$

since Lemma 4.7 (ii) implies $S = A + \mathfrak{p}S$, which in turn gives $F_i(a)S \subset F_i(a)A + \mathfrak{p}F_i(a)S \subset F_i(a)A + \mathfrak{p}S$.

If for some $i \neq j$ we had $\mathfrak{P}_i = \mathfrak{P}_j$, then, in view of $(f_i, f_j) = 1$ and the finiteness of k, there would exist polynomials $A, B \in R[X]$ and $C \in \mathfrak{p}[X]$ such that

$$A(X)F_i(X) + B(X)F_j(X) = 1 + C(X). \tag{4.4}$$

But $F_i(a) \in \mathfrak{P}_i$ and $F_j(a) \in \mathfrak{P}_j$, hence putting $X = a$ in (4.4) we obtain $1 \in \mathfrak{P}_i$, which is absurd.

Since the element

$$F_1(a)^{e_1} \cdots F_g(a)^{e_g} \tag{4.5}$$

belongs to $\mathfrak{p}S$, the prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are the only possible prime ideals dividing $\mathfrak{p}S$, and this shows that with suitable exponents $a_1, \ldots, a_g$ we must have $\mathfrak{p}S = \prod_{i=1}^{g} \mathfrak{P}_i^{a_i}$. The degree $f_{L/K}(\mathfrak{P}_i)$ equals $[k_i : k] = \deg f_i$, hence it remains to show that $e_i = a_i$ holds for $i = 1, 2, \ldots, g$. The ideal $\mathfrak{P}_i^{a_i}$ divides the product (4.5), but, as we have seen, $\mathfrak{P}_i$ can divide only the factor $F_i(a)^{e_i}$ of that product, thus $\mathfrak{P}_i^{a_i} | F_i(a)^{e_i} S$. It follows that the ideal $\mathfrak{p}S + F_i(a_i)^{e_i} S$ is divisible by $\mathfrak{P}_i^{a_i}$, but it divides $\mathfrak{P}_i^{e_i} S + F_i(a)^{e_i} S$, hence we must have $e_i \geq a_i$ for $i = 1, 2, \ldots, g$. Observe finally that Theorem 4.5 gives $\sum_{i=1}^{g} a_i \deg f_i = [L : K]$, and obviously $\sum_{i=1}^{g} e_i \deg f_i = [L : K]$, which together with the inequalities last obtained shows $a_i = e_i$. □

2. Now let us turn to applications of Theorem 4.33 to extensions of $\mathbb{Q}$. Lemma 4.32 (vi) shows that its assumptions are in this case satisfied by all prime ideals $p\mathbb{Z}$ of $\mathbb{Z}$ with at most finitely many exceptions, and the exceptional primes p are exactly those which divide the index of a. By varying a we may apply Theorem 4.33 to all primes p, except those which divide the indices of all integers. The possibility of such situation was already noted in Sect.2.2.5 and now we shall characterize such primes. It is useful to introduce the following definition: the greatest common divisor of indices of integers of K will be called the *index of* K, and denoted by $i(K)$.

If $a \in R_K$, then a rational prime p divides the index of a if and only if there exists a polynomial $V \in \mathbb{Z}[X]$ of degree not exceeding $[K : \mathbb{Q}] - 1$, whose coefficients are not all divisible by p, but p divides $V(a)$. This observation will be now used to establish the following theorem:

Theorem 4.34. *Let p be a rational prime, let*

$$pR_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

be the factorization of pR_K into prime ideals in an extension $K/\mathbb{Q}$ of degree n, and put $f_i = f_{K/\mathbb{Q}}(\mathfrak{P}_i)$. Then p does not divide the index $i(K)$ of K if and only if there exist distinct monic irreducible polynomials $V_1, \ldots, V_g$ over $\mathbb{F}_p$, satisfying $\deg V_i = f_i$ for $i = 1, 2, \ldots, g$.

Proof : If $p \nmid i(K)$, then there exists an integer a in K with its index not divisible by p, and Lemma 4.32 (vi) and Theorem 4.33 imply the existence of polynomials with required properties.

To prove the converse implication let $W_i \in \mathbb{Z}[X]$ be for $i = 1, 2, \ldots, g$ a polynomial, which after reduction mod p gives V_i, write $pR_K = \mathfrak{P}_i^{e_i} I_i$, and choose $a_i \in R_K$, generating the extension $K/\mathbb{Q}$ and satisfying

$$W_i(a_i) \equiv 0 \pmod{\mathfrak{P}_i}, \quad W_i(a_i) \not\equiv 0 \pmod{\mathfrak{P}_i^2}, \quad a_i \equiv 0 \pmod{I_i}.$$

To show that such choice is possible observe that the field $k_i = R_K/\mathfrak{P}_i$ is the only extension of $\mathbb{F}_p$ of degree f_i, hence every irreducible polynomial over $\mathbb{F}_p$ of degree f_i has a root in k_i. Therefore the congruence

$$W_i(X) \equiv 0 \pmod{\mathfrak{P}_i}$$

is solvable in R_K, and we may take for a_i one of its solutions. An irreducible polynomial over $\mathbb{F}_p$ cannot have multiple roots, hence if the condition $W_i(a_i) \notin \mathfrak{P}_i^2$ is not satisfied, then we may replace a_i by $a_i + \pi$, with $\pi \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$.

Now let $a \equiv a_i \pmod{\mathfrak{P}_i^2}$ for $i = 1, 2, \ldots, g$ be an element generating $K/\mathbb{Q}$ (which can be assured by Proposition 2.2 (ii)), and put $\mathfrak{Q}_i = pR_K + W_i(a)R_K$. We shall show that $\mathfrak{P}_i = \mathfrak{Q}_i$. Obviously we have $\mathfrak{P}_i | \mathfrak{Q}_i$ and $\mathfrak{P}_i^2 \nmid \mathfrak{Q}_i$, and, moreover, for $i \neq j$ we have $\mathfrak{P}_j \nmid \mathfrak{Q}_i$, since otherwise we would have

$$W_i(a) \equiv 0 \pmod{\mathfrak{P}_j}$$

and $W_i(a_j) \equiv 0 \pmod{\mathfrak{P}_j}$, but in view of $W_j(a_j) \equiv 0 \pmod{\mathfrak{P}_j}$ this would imply that V_i and V_j have a common root in k_j, which is not possible, since they are relatively prime. Since $\mathfrak{Q}_i$ divides pR_K, therefore it is not divisible by prime ideals different from $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$, and so we get $\mathfrak{P}_i = \mathfrak{Q}_i$. Now consider the polynomial $W = \prod_{i=1}^g W_i^{e_i}$. Clearly $W(a) \equiv 0 \pmod{pR_K}$.

Observe now that if $p | i(K)$, then for a suitable polynomial $S \in \mathbb{Z}[X] \setminus p\mathbb{Z}[X]$ with $\deg S \leq n-1$ we have $S(a) \equiv 0 \pmod{pR_K}$. Denote by $\overline{S}(X)$ the reduction mod p of $S(X)$, put $V(X) = \prod_{i=1}^g V_i^{e_i}(X)$, and let

$$D(X) = (V(X), \overline{S}(X)).$$

With suitable $A, B \in \mathbb{F}_p[X]$ we have

$$A(X)V(X) + B(X)\overline{S}(X) = D(X),$$

and so if $\hat{A}, \hat{B}, \hat{D} \in \mathbb{Z}[X]$ be polynomials whose reductions mod p are equal to A, B and D, respectively, then with certain $C(X) \in \mathbb{Z}[X]$ we get

$$\hat{A}(X)W(X) + \hat{B}(X)S(X) = \hat{D}(X) + pC(X),$$

and therefore $\hat{D}(a) \equiv 0 \pmod{pR_K}$. Since $D(X)$ divides $V(X)$ we get $D(X) = c\prod_{i=1}^g V_i(X)^{c_i}$ with $0 \leq c_i \leq e_i$ and some non-zero $c \in \mathbb{F}_p$, and thus with some $F(X) \in \mathbb{Z}[X]$, and $c' \in \mathbb{Z} \setminus p\mathbb{Z}$ we can write

$$\hat{D}(X) = c' \prod_{i=1}^g W_i(X)^{c_i} + pF(X).$$

Therefore $\mathfrak{P}_i^{e_i}$ divides $\prod_{i=1}^{g} W_i(a)^{c_i}$, and since for $i \neq j$ we have

$$(\mathfrak{P}_i, W_j(a)R_K) = 1,$$

we get $\mathfrak{P}_i^{e_i} | W_i^{c_i}(a)R_K$, leading to $c_i = e_i$ and $\hat{D} = W$. However $\deg \hat{D} \leq \deg S \leq n-1 < \deg W = n$, a contradiction. □

To apply the last theorem one has to know the number $r_p(n)$ of non-associated irreducible polynomials over $\mathbb{F}_p$ of degree n. This number was found by Gauss, and we now prove his formula:

Proposition 4.35. *For every prime p and $n \geq 1$ one has*

$$r_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}, \tag{4.6}$$

where $\mu(d)$ is the familiar Möbius function.

Proof : Consider the field $k = F_{p^n}$ which is of degree n over $\mathbb{F}_p$. Every irreducible polynomial over $\mathbb{F}_p$ of degree d dividing n has exactly d distinct roots in k. Noting that non-associated irreducible polynomials cannot have common zeros, we obtain

$$p^n = \#\mathbb{F}_{p^n} = \sum_{d|n} d r_p(d),$$

and the application of the Möbius inversion formula gives (4.6). □

The formula (4.6) permits us to bound the prime divisors of $i(K)$ from above:

Proposition 4.36. *If p is a prime dividing $i(K)$, then $p < [K : \mathbb{Q}]$.*

Proof : Let $1 \leq k \leq n = [K : Q]$. Among the degrees of prime ideals dividing pR_K there can be at most n/k equal to k. If $p | i(K)$ and $p \geq n$, then by Theorem 4.34 there must exist $k \leq n$ with $r_p(k) < n/k \leq p/k$. However, the sum on the right-hand side of (4.6) is non-zero and divisible by p, thus $r_p(k) \geq p/k$, a contradiction. □

Corollary. *If K is a cubic extension of $\mathbb{Q}$ and p is a prime divisor of $i(K)$, then $p = 2$. The prime 2 divides $i(K)$ if and only if one has $2R_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, with distinct prime ideals $\mathfrak{P}_i$.*

Proof : Observe that there are two irreducible linear polynomials over $\mathbb{F}_2$. □

Our next application of Theorem 4.33 deals with splitting primes:

Theorem 4.37. *If $K \subset L$ are algebraic number fields, then there are infinitely many prime ideals of R_K, splitting in R_L.*

Proof : It suffices to prove the assertion in the case $K = \mathbb{Q}$ and $L/\mathbb{Q}$ normal. In fact, if $M/\mathbb{Q}$ is a normal extension containing L, then Proposition 4.3 shows that if $p\mathbb{Z}$ splits in $M/\mathbb{Q}$, then every prime ideal of R_K, lying over $p\mathbb{Z}$ splits in L/K. Thus, using Theorem 4.33, we can reduce our assertion to the following form:

If $P \in \mathbb{Z}[X]$ is non-constant, then for infinitely many primes p the congruence $P(x) \equiv 0 \pmod{p}$ has a solution.

Assume this to be false for a certain polynomial P. Then its values can be divisible only by finitely many primes, say $p_1, \ldots, p_r$. Select x_0 with $|P(x_0)| \geq 2$, and write, with suitable non-negative a_i

$$P(x_0) = \epsilon \prod_{i=1}^{r} p_i^{a_i},$$

with $\epsilon = \pm 1$.

If now $M = \prod_{i=1}^{r} p_i^{a_i+1}$ and $x \equiv x_0 \pmod{M}$, then with suitable b_i we have

$$\epsilon \prod_{i=1}^{r} p_i^{a_i} = P(x_0) \equiv P(x) \pmod{M},$$

and if $|P(x)| = \prod_{i=1}^{r} p_i^{b_i}$, then we get $b_i = a_i$ for $i = 1, 2, \ldots, r$. Thus for infinitely many x we have $P(x) = \pm P(x_0)$, showing that P must be constant, a contradiction. □

We conclude this subsection with a result, which is often helpful in factorizing prime ideals. It is based on an extension of the notion of an Eisenstein polynomial. If $F(X) = a_n X^n + \cdots + a_0 \in R_K[X]$, and for a certain prime ideal $\mathfrak{p}$ of R_K we have $a_n \notin \mathfrak{p}$, $a_{n-1}, \ldots, a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$, then F is called *$\mathfrak{p}$-Eisensteinian*, or *Eisensteinian with respect to $\mathfrak{p}$*. In the same way as in the classical case $R_K = \mathbb{Z}$ one proves that such polynomial is irreducible over K.

Proposition 4.38. *If $a \in R_L$ generates the extension L/K, and its minimal polynomial $F(X) = X^n + \sum_{j=0}^{n-1} a_j X^j$ over R_K is $\mathfrak{p}$-Eisensteinian for a prime ideal $\mathfrak{p}$ of R_K, then $\mathfrak{p}$ ramifies completely in L/K, i.e., one has $\mathfrak{p}R_L = \mathfrak{P}^n$ with a certain prime ideal $\mathfrak{P}$ of R_L.*

Proof : Let $\mathfrak{P}$ be a prime ideal of R_L lying over $\mathfrak{p}$, and let $\mathfrak{P}^e$ be its highest power dividing $\mathfrak{p}R_L$. By Corollary 1 to Theorem 4.5 we have $e \leq n$, so it remains to establish the inequality $n \leq e$. From $a^n \in \mathfrak{p}R_L$ we infer $a \in \mathfrak{P}$, and, moreover, all coefficients a_i lie in $\mathfrak{P}^e$, so if we had $n \geq e + 1$, then the

ideal $\mathfrak{P}^{1+e}$ would contain $a_0 = -(a^n + \cdots + a_1 a)$ and we would have $a_0 \in \mathfrak{p}^2$, contrary to the assumption. □

3. We turn now to the principal applications of Theorem 4.33, namely to explicit factorizations of prime ideals. We start with quadratic fields:

Theorem 4.39. *Let K be a quadratic extension of the rationals with discriminant $d = d(K)$, and let p be a rational prime. If $p|d$, then we have $pR_K = \mathfrak{P}^2$, and if $p \nmid d$, then two cases arise:*

If p is odd, then

$$pR_K = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 & \text{if } \left(\frac{d}{p}\right) = 1, \\ \mathfrak{P} & \text{if } \left(\frac{d}{p}\right) = -1, \end{cases}$$

and if $p = 2$, then

$$2R_K = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 & \text{if } d \equiv 1 \pmod 8, \\ \mathfrak{P} & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

Proof : If D is the square-free part of d, i.e., $D = d$ if $d \equiv 1 \pmod 4$ and $D = d/4$ otherwise, then $\sqrt{D}$ generates K, and in view of Theorem 2.18 its index equals either 1 or 2, the last case arising if $d \equiv 1 \pmod 4$. As the minimal polynomial for $\sqrt{D}$ equals $X^2 - D$, our assertion concerning odd primes p follows immediately from Theorem 4.33, and the same happens for $p = 2$, provided $4|d$. The remaining case ($p = 2$ and $d \equiv 1 \pmod 4$) requires the observation that $(1 + \sqrt{D})/2$ has index 1, and its minimal polynomial equals $X^2 - X + (1 - D)/4$, which is irreducible over $\mathbb{F}_2$ if and only if D is congruent to 5 mod 8. □

Now we consider cyclotomic fields.

Theorem 4.40. *Let $K = \mathbb{Q}(\zeta_m)$ with $m \not\equiv 2 \pmod 4$, and let p be a rational prime.*

If $p \nmid m$ and f is the order of $p \bmod m$, i.e., the least positive integer with $p^f \equiv 1 \pmod m$, then pR_K is the product of $\varphi(m)/f$ distinct prime ideals of R_K having degree f.

If $p|m$, $m = p^a m_1$, with $p \nmid m_1$, and f_1 is the order of $p \bmod m_1$, then

$$pR_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e,$$

with $e = \varphi(p^a)$, $g = \varphi(m_1)/f_1$ and distinct prime ideals $\mathfrak{P}_i$'s of degree f_1.

Proof : We start with a lemma, which is also applicable in a more general situation:

Lemma 4.41. *Let K be an algebraic number field, not containing the m-th primitive root of unity ζ_m and let $L = K(\zeta_m)$. Put $n = [L : K]$, and let $\mathfrak{p}$ be a prime ideal of R_K, not containing m and of the first degree over $\mathbb{Q}$. If f is the order of $N(\mathfrak{p}) \bmod m$, then in L we have the decomposition*

$$\mathfrak{p}R_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g,$$

with $g = n/f$ and all prime ideals $\mathfrak{P}_i$ distinct and of degree f over K.

Proof : Since the extension L/K is normal and $\mathfrak{p}$ is unramified, we have only to show that the degree of any prime ideal $\mathfrak{P}$, lying over $\mathfrak{p}$ in L, equals f. Put $A = R_K[\zeta_m]$ and observe that the conductor $\mathfrak{f}$ of A divides mR_L. Indeed, if $F \in R_K[X]$ is the minimal polynomial of ζ_m, then there exists $G \in R_K[X]$ such that $F(X)G(X) = X^m - 1$, and this shows

$$\delta_{L/K}(\zeta_m)G(\zeta_m) = m\zeta_m^{m-1}.$$

Since ζ_m is a unit, we see that $\delta_{L/K}(\zeta_m)R_L$ divides mR_L, and Proposition 4.18(i) gives now $\mathfrak{f}|mR_L$. Therefore $N_{L/K}(\mathfrak{f})|m^n R_K$, and we obtain that $\mathfrak{p}$ satisfies the condition (v) of Lemma 4.32. Hence for every $x \in R_L$ there is a polynomial $V \in R_K[X]$, such that

$$x \equiv V(\zeta_m) \pmod{\mathfrak{p}R_L}. \tag{4.7}$$

From the properties of multinomial coefficients we obtain now

$$x^{N(\mathfrak{p})^f} \equiv V(\zeta_m)^{N(\mathfrak{p})^f} \equiv V(\zeta_m^{N(\mathfrak{p})^f}) \equiv V(\zeta_m) \equiv x \pmod{\mathfrak{p}R_L},$$

and clearly the same congruence holds also mod $\mathfrak{P}$. Put $t = f_{L/K}(\mathfrak{P})$ and use Theorem 1.18 to obtain that $N(\mathfrak{P}) = N(\mathfrak{p})^t$ is the minimal exponent $r > 1$ for which $y^r \equiv y \pmod{\mathfrak{P}}$ holds for all $y \in R_L$. This forces $t \leq f$. If we would have $N(\mathfrak{p})^t \not\equiv 1 \pmod{m}$, then $\zeta_m^{N(\mathfrak{p})^t}$ would be a primitive m-th root of unity different from ζ_m, and so the difference $\zeta_m^{N(\mathfrak{p})^t} = \zeta_m$ would lie in $\mathfrak{P}$. This would imply in turn that the discriminant of the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ lies in $\mathfrak{P} \cap \mathbb{Z}$, but this ideal is generated by a rational prime not dividing m, in contradiction to Theorem 4.27. Hence $N(\mathfrak{p})^t \equiv 1 \pmod{m}$, thus $f \leq t$ and we obtain $t = f$. □

Our assertion concerning primes not dividing m follows immediately from the lemma. The case $p|m$ is more complicated. Denote by K_1 the field $\mathbb{Q}(\zeta_{m_1})$ and put $q = p^a$. Since $[K : \mathbb{Q}] = \varphi(m)$ and $[K_1 : \mathbb{Q}] = \varphi(m_1)$, it follows that

$$[K : K_1] = \varphi(m)/\varphi(m_1) = \varphi(q) = [\mathbb{Q}(\zeta_q) : \mathbb{Q}],$$

and we see that the q-th cyclotomic polynomial $F_q(X)$ is irreducible over K_1. Since p does not divide m_1 we may apply the already proved part of the theorem to the field K_1, and obtain

$$pR_{K_1} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

with distinct prime ideals $\mathfrak{p}_i$ and $g = \varphi(m_1)/f$. In K we have the factorization

$$pR_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^e,$$

with some s and e to be determined. But we know that

$$sef_{K/\mathbb{Q}}(\mathfrak{P}_i) = [K : \mathbb{Q}] = \varphi(m) = \varphi(m_1)\varphi(q), \tag{4.8}$$

and since p is not ramified in $K_1/\mathbb{Q}$, we must have

$$e|[K : K_1] = \varphi(q).$$

Consider now the following factorization of the prime p in K:

$$p = F_q(1) = \prod_k (1 - \zeta_q^k) = (1 - \zeta_q)^{\varphi(q)} \prod_k (1 + \zeta_q + \cdots + \zeta_q^{k-1}),$$

where both products are taken over integers from the interval $[1, q]$, not divisible by p. The number $1 - \zeta_q$ is not a unit, hence the second product occurring in the last equality must be a unit, as p cannot be factorized in more that $\varphi(q)$ non-unit factors in the field $\mathbb{Q}(\zeta_q)$. Denoting this unit by ϵ, we arrive finally at

$$p = \epsilon(1 - \zeta_q)^{\varphi(q)},$$

and so

$$pR_K = (1 - \zeta_q)^{\varphi(q)} R_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^e.$$

Since $e|\varphi(q)$, we obtain $e = \varphi(q)$, and (4.8) leads us to $sf_{K/\mathbb{Q}}(\mathfrak{P}_i) = \varphi(m_1)$, hence $f_{K/\mathbb{Q}}(\mathfrak{P}_i) = \varphi(m_1)/s$. In view of

$$f_{K/\mathbb{Q}}(\mathfrak{P}_i) \geq f_{K_1/\mathbb{Q}}(\mathfrak{p}_i) = f_1$$

we arrive finally at $s \leq \frac{\varphi(m_1)}{f_1} = g$, and $s = g$. □

For later reference we state separately the factorization of the prime p in $\mathbb{Q}(\zeta_{p^a})$, obtained in the last theorem:

Corollary. *If p is a prime and $a \geq 1$, then in $K = \mathbb{Q}(\zeta_{p^a})$ we have $pR_K = \mathfrak{P}^e$, where $e = \varphi(p^a)$, and $\mathfrak{P}$ is the principal ideal generated by $1 - \zeta_{p^a}$.* □

As the third example we consider *Kummerian extensions*, i.e., extensions $L = K(a)$ of a field K containing all n-th roots of unity, with a being a root of an irreducible polynomial of the form $X^n - c$ with $c \in K$. Such extensions are always cyclic, and every cyclic extension of degree n of a field containing the n-th roots of unity must necessarily be of this form. The proof of this fact can be found in any textbook of Galois theory.

Theorem 4.42. *Let L/K be a Kummerian extension of degree n, generated by $a \in R_L$ with $a^n = c \in R_K$. Moreover, let $\mathfrak{p}$ be a prime ideal of R_K, not containing cn and define r as the maximal divisor of n, for which the congruence*

$$X^r \equiv c \pmod{\mathfrak{p}}$$

has a solution in R_K. Then $\mathfrak{p}R_L$ is a product of r distinct prime ideals.

Proof : We need first a simple lemma:

Lemma 4.43. *Let $k = R_K/\mathfrak{p}$ and $k' = R_L/\mathfrak{P}$, where $\mathfrak{P}$ is a prime ideal of R_L, lying above $\mathfrak{p}$. Denote by $\bar{a}$ the image of a in k' and let t be a divisor of n. If $u = n/t$, then the congruence*

$$X^t \equiv c \pmod{\mathfrak{p}}$$

has a solution in R_K if and only if the element $b(a) = (\bar{a})^u$ lies in k.

Proof : If $b(a) \in k$, then every element of R_K lying in the residue class $b(a)$ satisfies our congruence. Conversely, if $x \in R_K$ satisfies $x^t \equiv c \bmod \mathfrak{p}$, and $\bar{x}$ denotes the image of x in k, then $\bar{c} = (\bar{a})^n = b(a)^t$, whence $(\bar{x}/b(a))^t = 1$. But the finite field k contains all t-th roots of unity since by our assumption K contains the splitting field of $X^n - 1$. Thus $\bar{x}/b(a) \in k$ and $b(a) \in k$. □

We retain the notation of the lemma. Let f be the minimal positive exponent with $\bar{a}^f = u \in k$, and observe that the polynomial $X^f - u$ is irreducible over k. In fact, if $n = Af + B$ with $0 \leq B < f$, then $\bar{a}^B \in k$, thus $B = 0$. Hence f divides n, and k contains a primitive f-th root of unity, say w. Since

$$X^f - u = X^f - \bar{a}^f = \prod_{i=0}^{f-1} (X - \bar{a}w^i),$$

the constant term of any presumable factor of $X^f - c$ would have the form $\pm\bar{a}^u y$ with $y \in k$ and $1 \leq u < f$. But our choice of f gives $u = f$, and thus our polynomial is irreducible. Since a root of it generates the extension k'/k, we obtain $f_{L/K}(\mathfrak{P}) = [k' : k] = f$, and the application of Lemma 4.43 concludes the proof of the theorem. □

4. The knowledge of factorization of prime ideals of $\mathbb{Z}$ in an extension $K/\mathbb{Q}$ is very helpful in determining the class-number of K and the structure of its class-group $H(K)$. We shall illustrate this on the examples which follow.

First we consider imaginary quadratic fields:

Proposition 4.44. *Imaginary quadratic fields with discriminants $d = -3$, -4, $-7, -8$, $-11, -19$, $-43, -67$ and -163 have a trivial class group.*

Proof : For $d = -3, -4, -7, -8$ this is an immediate consequence of Lemma 3.8. In the remaining cases we again use this lemma. According to it in every class of ideals in the considered fields there is an ideal whose absolute norm does not exceed $2/\pi\sqrt{|d|} < 0.63662\sqrt{|d|}$. Applying this to $d = -11, -19, -43, -67, -163$ we obtain the bounds $2, 2, 4, 5$ and 8, respectively. Since our discriminants are all congruent to $5 \bmod 8$, Theorem 4.39 shows that the number 2 generates a principal prime ideal, and therefore we obtain $h = 1$ in the first two cases. For $d = -43$ we have to consider ideals of norm 3 and 4, but Theorem 4.39 shows that $3R_K$ is a prime ideal, and therefore there are no ideals of norm 3, and $2R_K$ is the unique ideal of norm 4. This proves $h = 1$ for $d = -43$. In the remaining two cases our assertion results in the same way from

$$\left(\frac{-67}{3}\right) = \left(\frac{-67}{5}\right) = -1,$$

and

$$\left(\frac{-163}{p}\right) = -1$$

for $p = 3, 5, 7$. □

It is much more difficult to prove that those fields are the only imaginary quadratic fields with class-number one.

To obtain a less trivial example of the class-group consider the field $K = \mathbb{Q}(\sqrt{-14})$ of discriminant -56. Lemma 3.8 shows that every its class of ideals contains an ideal of absolute norm not exceeding 4. Theorem 4.39 implies $2R_K = \mathfrak{p}_2^2$ with a prime ideal $\mathfrak{p}_2$, which is not principal, since $N(\mathfrak{p}_2) = 2$, and there are no principal ideals in R_K having norm 2, because of

$$N_{K/Q}(x + y\sqrt{-14}) = x^2 + 14y^2 \neq 2$$

for $x, y \in \mathbb{Z}$. For the same reason we get $3R_K = \mathfrak{p}_3\mathfrak{p}_3'$ with non-principal ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$. Finally, the only ideal of norm 4 is $2R_K$, which is principal. Therefore the set $\{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'\}$ represents all non-principal classes, thus $2 \leq h \leq 4$. Denote by X, Y the ideal classes containing $\mathfrak{p}_2$ and $\mathfrak{p}_3$, respectively, and let E be the principal class. If we had $X = Y$, then in view of $X^2 = E$ the product $\mathfrak{p}_2\mathfrak{p}_3$ would be principal, but its norm equals 6, and 6 is not represented by the form $x^2 + 14y^2$, so $\mathfrak{p}_2\mathfrak{p}_3$ is not principal, hence $X \neq Y$. Therefore there are at least 3 distinct classes, namely E, X and Y. Since X is of order 2 we must have $h = 4$, hence $H(K) = \{E, X, Y, Z\}$, where $Z = Y^{-1}$ is the class containing $\mathfrak{p}_3'$. In view of $Y \neq Y^{-1}$ we see that $H(K)$ is cyclic.

A similar argument can be applied also to real quadratic fields. However. in this case additional difficulties arise, connected with testing the existence of principal ideals of a given norm. We illustrate this on the example of $K = \mathbb{Q}(\sqrt{10})$ with $d(K) = 40$. Lemma 3.8 shows that we have to look at ideals

of norms 2 and 3. By Theorem 4.39 we have $2R_K = \mathfrak{p}_2^2$ and $3R_K = \mathfrak{p}_3\mathfrak{p}_3'$. The ideals $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ are not principal, since the equation $x^2 - 10y^2 = a$ does not have rational integral solutions for $a = \pm 2, \pm 3$, because 2 and 3 are quadratic non-residues mod 5. If X, Y, Z are ideal classes, containing $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, respectively, then we have $X^2 = ZY = E$. Now observe that the only ideals with norm 6 are $\mathfrak{p}_2\mathfrak{p}_3 \in XY$ and $\mathfrak{p}_2\mathfrak{p}_3' \in XZ = XY^{-1}$. It happens that the principal ideals generated by $4+\sqrt{10}$ and $4-\sqrt{10}$ are both of norm 6, and are distinct, the ratio $(4+\sqrt{10})/(4-\sqrt{10})$ being not integral. This establishes $XY = E$ and $XY^{-1} = E$, and so finally we see that $X = Y = Y^{-1}$, hence $H(K) = C_2$.

In the general case one has to determine whether a quadratic form represents a given integer, and this may be sometimes rather an awkward task.

Now we consider a few pure cubic fields $K = \mathbb{Q}(\sqrt[3]{m})$ with m square-free and not congruent to ± 1 mod 9. Theorem 2.19 shows that in this case the discriminant equals $-27m^2$, the index of $\theta = \sqrt[3]{m}$ equals 1, and Lemma 3.8 shows that every ideal class contains an ideal of norm smaller than $3m/2$. Moreover a simple computation shows that

$$N_{K/\mathbb{Q}}(x + y\theta + z\theta^2) = x^3 + my^3 + m^2z^3 - 3xyzm. \tag{4.9}$$

If $m = 2$, then we have to check only ideals of norm 2, but the polynomial $X^3 - 2$ is a third power mod 2, hence Theorem 4.33 gives $2R_K = \mathfrak{p}^3$ and since $\mathfrak{p}$ is generated by θ we get $h = 1$.

If $m = 3$, then we have to consider ideals of norms ≤ 4. In view of

$$X^3 - 3 \equiv (X-1)(X^2 + X + 1) \,(\mathrm{mod}\ 2) \quad \text{and} \quad X^3 - 3 \equiv X^3 \,(\mathrm{mod}\ 3)$$

we get $2R_K = \mathfrak{p}_2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = 2$, $N(\mathfrak{p}_2') = 4$, and $3R_K = \mathfrak{p}_3^3$ with $N(\mathfrak{p}_3) = 3$. In view of $N_{K/\mathbb{Q}}(\theta - 1) = 2$ we get $\mathfrak{p}_2 = (\theta - 1)R_K$, hence $\mathfrak{p}_2$ and $\mathfrak{p}_2' = (2R_K)\mathfrak{p}_2^{-1}$ are both principal. Since $\mathfrak{p}_3$ is generated by θ we obtain $h = 1$ also in this case. By the same method one shows that for $m = 5$ and $m = 6$ one obtains fields with a trivial class-group.

Now consider $m = 7$. Here we have to check ideals with norms ≤ 10. Factorizing the polynomial $X^3 - 7$ in $\mathbb{F}_p$ for $p = 2, 3, 5$ and 7 we obtain

$$\begin{aligned} 2R_K &= \mathfrak{p}_2\mathfrak{p}_2' \quad \text{with} \quad N(\mathfrak{p}_2) = 2, N(\mathfrak{p}_2') = 4, \\ 3R_K &= \mathfrak{p}_3^3 \quad \text{with} \quad N(\mathfrak{p}_3) = 3, \\ 5R_K &= \mathfrak{p}_5\mathfrak{p}_5' \quad \text{with} \quad N(\mathfrak{p}_5) = 5, N(\mathfrak{p}_5') = 25, \\ 7R_K &= \mathfrak{p}_7^3 \quad \text{with} \quad N(\mathfrak{p}_7) = 7. \end{aligned}$$

Now observe that every cube of a rational integer is either divisible by 7 or is congruent to $\pm 1 \,(\mathrm{mod}\ 7)$, hence it follows from (4.9) that every norm of an integer of K is congruent to 0, 1 or -1 mod 7, and therefore the ideals $\mathfrak{p}_2, \mathfrak{p}_2'$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, and $\mathfrak{p}_5'$ are non-principal. The ideal $\mathfrak{p}_7$ is obviously principal, being generated by θ. Let X be the ideal class containing $\mathfrak{p}_3$. Then $X^3 = E$, E being the unit class. It follows from (4.9) that $N_{K/\mathbb{Q}}(1 - \theta) = -6$ and

$N_{K/\mathbb{Q}}(2+\theta) = 15$ and therefore the products $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_3\mathfrak{p}_5$ are both principal. Thus $\mathfrak{p}_2 \in X^{-1} = X^2$ and $\mathfrak{p}_5 \in X^2$, implying $\mathfrak{p}_2' \in X$. This shows that every tested prime ideal lies in the cyclic subgroup of $H(K)$ generated by X. But every other ideal yet to be tested is a product of those prime ideals, and so $H(K)$ coincides with this subgroup, i.e. $h = 3$ and $H(K) = C_3$.

Now we consider a sample of cyclotomic fields.

Proposition 4.45. *Cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$ with $m \leq 8$ have a trivial class-group.*

Proof : The cases $m = 3, 4, 6$ are covered by the preceding proposition, and in the case $m = 5$ the assertion is an immediate consequence of Lemma 3.8, since the Minkowski constant in this case is less than 2. For $m = 7$ we have to consider ideals with norms ≤ 4. Since the number 3 generates a prime ideal and $2R_K = \mathfrak{p}\mathfrak{q}$ with $N(\mathfrak{p}) = N(\mathfrak{q}) = 8$, hence again we get $h = 1$. Finally, in the case $m = 8$ we have to test ideals of norm ≤ 2. Theorem 4.33 gives $2R_K = \mathfrak{p}_2^4$, $N(\mathfrak{p}_2) = 2$, and it follows from the Corollary to Theorem 4.40 that $\mathfrak{p}_2$ is principal. Thus also in this case the class-group is trivial. □

5. We conclude this section with some results concerning the behaviour of the class-group under extensions. As we already have seen, an embedding $K \subset L$ induces a monomorphism $i_{L/K}$ of the group of fractional ideals $G(K)$ into $G(L)$, which maps principal ideals into principal ideals. This induces in turn a homomorphism of the class-group $H(K)$ in $H(L)$, which we shall denote by $i^*_{L/K}$. Immediately from the definition follows the following proposition:

Proposition 4.46. *(i) The map $i^*_{L/K}$ is injective if and only if no non-principal ideal of K is mapped by $i^*_{L/K}$ on a principal ideal of L.*

(ii) The map $i^*_{L/K}$ is surjective if and only if to every fractional ideal I of L there corresponds a non-zero element $a \in L$ and an ideal J of R_K such that $I = aJR_L$.

(iii) The map $i^*_{L/K}$ is trivial if and only if every fractional ideal of K becomes a principal ideal in L. □

The following theorem, in a quite different formulation, was used by Kummer for founding his theory of ideal numbers:

Theorem 4.47. *Every algebraic number field K has an extension L/K with $[L : K] \leq h(K)$ and trivial $i^*_{L/K}$.*

Proof : Let

$$H(K) = C_{h_1} \times \cdots \times C_{h_r}$$

be a factorization of $H(K)$ with cyclic factors, and let, for $j = 1, 2, \ldots, r$, X_j be a generator of the group C_{h_j}. For each $j = 1, 2, \ldots, r$ choose an ideal I_j in

X_j. Then the ideal $I_j^{h_j}$ is principal, so let $a_j \in R_K$ be its generator, and let b_j be a root of the polynomial $X^{h_j} - a_j$. Denote by L the field $K(b_1, \ldots, b_r)$, and observe that $[L : K] \leq h_1 h_2 \cdots h_r = h$. Now let $I \in R_K$ be a non-principal ideal, and let

$$X = X_1^{m_1} \cdots X_r^{m_r}$$

be the class to which it belongs. Then the fractional ideal $I \prod_{j=1}^{r} I_j^{-m_j}$ is principal, generated by, say $a \in K$. Now observe that for $j = 1, 2, \ldots, r$ we have

$$(b_i R_L)^{h_i} = a_i R_L = I_i^{h_i} R_L,$$

thus $I_i R_L = b_i R_L$. This implies

$$IR_L = \left(a \prod_{j=1}^{r} I_j^{m_j} \right) R_L = a \prod_{j=1}^{r} b_j^{m_j} R_L,$$

hence I becomes principal in L. □

Now we define the norm-homomorphism for ideal classes. Since the map $N_{L/K}$ carries principal ideals into principal ideals, it induces a homomorphism of the corresponding class-groups, which we shall again denote by $N_{L/K}$. By Proposition 4.7 (v) we get $N_{L/K} \circ i^*_{L/K}(X) = X^n$, where n is the degree of L/K. Moreover, we immediately obtain from the definition the following properties of the norm map:

Proposition 4.48. *(i) The map $N_{L/K}$ is injective if and only if every non-principal ideal has a non-principal norm.*

(ii) The map $N_{L/K}$ is surjective if and only if for every ideal I of R_K there exists a non-zero $a \in K$ such that the ideal aI is the norm of a fractional ideal of L.

(iii) The map $N_{L/K}$ is trivial if and only if the norm of every ideal of R_L is principal. □

In a similar way one defined the analogous homomorphisms of the narrow class groups.

For prime p denote by $H_p(K)$ the p-component of the group $H(K)$.

Proposition 4.49. *Let $n = [L : K]$ and let p be a prime not dividing n. Then*

(i) The map $i^*_{L/K}$ restricted to $H_p(K)$ is an embedding of $H_p(K)$ into $H_p(L)$.

(ii) The map $N_{L/K}$ restricted to $H_p(L)$ maps this group onto $H_p(K)$.

Proof : (i) If the class X lies in $H_p(K) \cap$ Ker $i^*_{L/K}$, then

$$X^n = N_{L/K}(i^*_{L/K}(X)) = E,$$

but the order of X is a power of p, and in view of $p \nmid n$ we get $X = E$.

(ii) Let $X \in H_p(K)$ and let p^r be its order. There exist rational integers A, B with $Ap^r + Bn = 1$. Then $N_{L/K}(i^*_{L/K}(X^B)) = X^{Bn} = X$. □

Corollary 1. *If the class-number $h(K)$ is prime to the degree of L/K, then the map $i^*_{L/K}$ is injective and $h(K)$ divides $h(L)$.* □

Corollary 2. *If $p \nmid n = [L : K]$, then $H_p(L)$ is the direct product of $H_p(K)$ and* Ker $N_{L/K} \cap H_p(L)$, *and if $(h(K), n) = 1$, then $H(L) = H(K) \times$* Ker $N_{L/K}$.* □

In the case of a cyclic class-group $H(K)$ one can improve part (ii) of the last proposition, yielding the following counterpart to Theorem 4.47:

Theorem 4.50. *If $H(K)$ is cyclic, and L is a field containing K in which every ideal of K becomes principal, then $h(K)$ divides $[L : K]$, hence $[L : K] \geq h(K)$.*

Proof : We need an auxiliary result:

Lemma 4.51. *Let p be a prime and let C_{p^a} be a cyclic factor of $H_p(K)$. If $[L : K] = n = p^b N$ with $p \nmid N$, then the group $i^*_{L/K}(C_{p^a})$ is cyclic, and has at least p^{a-b} elements.*

Proof : If X be a generator of C_{p^a}, then obviously $i^*_{L/K}(X)$ is a generator of the group $i^*_{L/K}(C_{p^a})$. If this group has p^c elements, then

$$X^{Np^{b+c}} = X^{np^c} = N_{L/K}(i^*_{L/K}(X^{p^c})) = E,$$

and thus $b + c \geq a$ and $c \geq a - b$, as asserted. □

The assumptions of the theorem imply that for every prime p the image $i^*_{L/K}(H_p(K))$ is trivial. Writing $[L : K] = p^b N$ with $p \nmid N$ and $H_p(K) = C_{p^a}$ we obtain from the lemma the inequality $a \leq b$, thus $h(K)$ divides $[L : K]$, as asserted. □

It should be pointed out that Theorem 4.50 may fail if $H(K)$ is not cyclic. We demonstrate this on an example due to Furtwängler [16]: consider the field $K = \mathbb{Q}(\sqrt{-21})$. We shall show that $H(K) = C_2 \times C_2$, thus $h(K) = 4$, but every ideal of R_K becomes principal in three quadratic extensions of K, namely in $L_1 = K(\sqrt{-3})$, $L_2 = K(\sqrt{-7})$ and $L_3 = K(\sqrt{21})$. The discriminant of K equals -84, hence Lemma 3.8 shows that we have to test

ideals of norms not exceeding 6. By Theorem 4.39 we obtain $2R_K = \mathfrak{p}_2^2$, $3R_K = \mathfrak{p}_3^2$ and $5R_K = \mathfrak{p}_5\mathfrak{p}_5'$. Since the norms of prime ideals occurring here, namely $2, 3$ and 5, cannot be expressed in the form $a^2 + 21b^2$, none of them is principal. For the same reason the products $\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\mathfrak{p}_5$, $\mathfrak{p}_2\mathfrak{p}_5'$, $\mathfrak{p}_3\mathfrak{p}_5$ and $\mathfrak{p}_3\mathfrak{p}_5'$ are non-principal. Let X, Y, Z, T be the ideal classes containing $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ and $\mathfrak{p}_5'$, respectively. Then $X^2 = Y^2 = ZT = E$, and X, Y, Z are distinct, thus $h(K) \geq 4$. On the other hand, evidently $h(K) \leq 5$, and since $h(K)$ is even, X being of order 2, we obtain $h(K) = 4$, and we see that $H(K)$ is non-cyclic, generated by X and Y. It remains to prove that in the fields L_1, L_2 and L_3 the ideals $\mathfrak{p}_2$ and $\mathfrak{p}_3$ become principal, but this is implied by the following decompositions:

$$\begin{aligned} 2 &= (8 + 3\sqrt{7})(3 - \sqrt{7})^2, \quad 3 = -(\sqrt{-3})^2 \quad \text{in } L_1, \\ 2 &= (2 - \sqrt{3})(1 + \sqrt{3})^2, \quad 3 = (\sqrt{3})^2 \quad \text{in } L_2, \end{aligned}$$

$$2 = -i(1+i)^2, \quad 3 = \left(\frac{5 - \sqrt{21}}{2}\right)\left(\frac{3 + \sqrt{21}}{2}\right)^2 \quad \text{in } L_3,$$

and the observation that the numbers

$$8 + 3\sqrt{7}, 2 - \sqrt{3}, -i, (5 - \sqrt{21})/2$$

are units.

6. Finally consider a normal extension L/K with Galois group G. This group acts on the group of fractional ideals of L, and since the subgroup consisting of all principal ideals is invariant under G, hence G acts also on the group $H(L)$ of ideal classes. A class $A \in H(L)$ is called *ambiguous* if it is invariant under G, and obviously the set of all ambiguous classes forms a group, which we shall denote by $Am(L/K)$, and call the *group of ambiguous ideal classes*. For prime p we shall denote by $Am_p(L/K)$ the p-component of $Am(L/K)$.

Observe that the image of $H(K)$ in $H(L)$ under the map $i^*_{L/K}$ is contained in $Am(L/K)$. It may happen, however, that this image does not cover the full group $Am(L/K)$, as may be seen from the following example: let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-14})$. We showed earlier that $H(L) = C_4$ and the only prime ideal dividing $2R_L$ lies in a class X, generating $H(L)$. This ideal is invariant under the action of the Galois group, and so the class X is ambiguous, but it does lie in the image of the trivial class-group of K.

In some cases it is possible to say more about $Am(L/K)$.

Proposition 4.52. *Let L/K be normal of degree n. Then*

(i) If $(n, h(K)) = 1$, then $i^*_{L/K}(H(K))$ is a direct factor of $Am(L/K)$.

(ii) If $(n, h(K)) = (n, h(L)) = 1$, then $Am(L/K) = i^*_{L/K}(H(K)) \sim H(K)$.

(iii) If $n = p^a$ is a prime power, $p \nmid h(K)$ and $Am(L/K) \sim i^*_{L/K}(H(K))$, then $p \nmid h(L)$, and the quotient $h(L)/h(K)$ is a rational integer, congruent to unity mod p.

Proof : (i) From the proof of part (ii) of Proposition 4.49 one can readily see that our assumptions imply

$$N_{L/K} \circ i^*_{L/K}(H(K)) = H(K).$$

We infer in turn that the map

$$f = i^*_{L/K} \circ N_{L/K} : \ Am(L/K) \longrightarrow Am(L/K)$$

is an endomorphism with image $i^*_{L/K}(H(K))$. The kernel of f equals

$$\{X \in Am(L/K) : \ X^n = E\},$$

because for ambiguous X we have $f(X) = i^*_{L/K}(X^n)$. Since $i^*_{L/K}(H(K))$ and Ker f have their orders relatively prime, we see that the extension

$$1 \longrightarrow \text{ Ker } f \longrightarrow Am(L/K) \longrightarrow i^*_{L/K}(H(K)) \longrightarrow 1$$

splits.

(ii) It suffices to observe that Ker f must be trivial in our case and apply (i).

(iii) Observe first that if a finite p-group G acts on a finite Abelian group H as a group of endomorphisms, then $\#H$ is congruent mod p to the number of its elements which are invariant under G. To see this let $o(h)$ be the orbit of an element $h \in H$ under the action of G, i.e., $o(h) = \{g(h) : \ g \in G\}$. If h is G-invariant, then $\#o(h) = 1$ and otherwise $\#o(h)$ is divisible by p, and so

$$\#H \equiv \sum_{\substack{h \\ \#o(h)=1}} 1 \pmod{p}.$$

Applying this observation to our situation, we see first that $h(L)$ is congruent to $\#Am(L/K)$ mod p, and since $\#Am(L/K) = h(K)$, we obtain $p \nmid h(L)$. The quotient $h(L)/h(K)$ is a rational integer by Corollary 1 to Proposition 4.49, and for the same reason we have $H(K) \subset H(L)$. Now observe that the quotient group $H(L)/H(K)$ has no non-trivial elements invariant under $G = Gal(L/K)$. Indeed, otherwise there would exist a class $X \in H(L)$ such that for every $g \in G$ we have $g(X) = XY_g$, with $Y_g \in i^*_{L/K}(H(K)$. If g is a non-trivial element of G, and p^k is its order, then we get

$$X = g^{p^k}(X) = XY_g^{p^k},$$

thus Y^{p^k} is the unit class E, and since $p \nmid h(L)$, we infer that $Y_g = E$. Therefore $g(X) = X$ holds for every $g \in G$, implying $X \in Am(L/K) =$

$H(K)$. The preceding argument shows now that the order of $H(L)/H(K)$ has to be congruent to unity mod p. □

If $(n, h(K)) > 1$, then similar results hold for the groups $H_p(K)$, $H_p(L)$ and $Am_p(L/K)$ for every prime $p \nmid n$. In particular one has the following result:

Corollary. *If L/K is normal of degree n and p is a prime not dividing n, then the groups $H_p(K)$ and $H_p(L)$ are isomorphic if and only if every class of $H_p(L)$ is ambiguous.* □

4.4. Notes to Chapter 4

1. The main results of this chapter are due to Dedekind [71], [78]. Theorem 4.10 was proved in Landau [18a], and another bound appears in Newman [56]. The evaluation of the class-number is closely connected with that of the regulator, since, as proved by Siegel [36] for quadratic fields and by Brauer [47a] in the general case, for fields K of a fixed degree one has

$$|d(K)|^{1/2-\epsilon} \leq R(K)h(K) \leq |d(K)|^{1/2+\epsilon}$$

for all $\epsilon > 0$ and sufficiently large $|d(K)|$. We shall establish this result for Abelian fields in Chap. 8 (see Theorem 8.14). In that chapter more information will be given about the asymptotical behaviour of the class-number.

For the minimal field K for which a given ideal $I \subset R_L$ lies in the image of $i_{L/K}$ see Mann [50].

2. Theorem 4.11 was proved by Pellet [78], and later rediscovered by Stickelberger [97], Voronoi [04] and Skolem [52]. See also Carlitz [53c] (where a similar result was obtained for $p = 2$), Cvetkov [83], Dalen [55], Hensel [05b], Herbrand [32d], Lasker [16] and Swan [62].

The definition and principal properties of the different and conductor appear in Dedekind [78], where one finds in particular Theorem 4.16, Proposition 4.18 and Lemma 4.19. Ideals which can serve as conductors were characterized in Dedekind [82] (cf. Furtwängler [19], Grell [27]). For other results on conductors see Bauer [36], Hensel [87], Ore [27].

Proposition 4.13 (iv) appears first in Hecke [17b], and for Corollaries 1 and 2 to it see Halter-Koch [67] and Yokoi [60]. We shall see later that if L/K is tame, then the trace map $R_L \longrightarrow R_K$ is surjective, and the converse holds for normal extension (see Corollary 3 to Proposition 6.2). More generally, if L/K is tame, then for every ideal I of R_K one has $T_{L/K}(I) = I \cap R_K$ (Ullom [69]). Proposition 4.17 goes essentially back to Euler. Possible forms of the discriminant $d(L/K)$ were determined in Ore [27] and W.R.Thompson [31].

3. Theorem 4.22 was stated by Weil [43] and a proof was published by Kawada [51]. The proof given here, as well as that of the different theorem (Theorem 4.24), is a modification of that of Kawada (cf. Kinohara [52], Narkiewicz [69], Neukirch [67]).

The first proof of the different theorem was given by Dedekind [82]. For other proofs of that theorem, or of the discriminant theorem (Corollary 2 to Theorem 4.24) see Artin [59], [67], Bauer [23], Chebotarev [37b], Hecke [23], Hensel [94a], Hilbert [97], Narkiewicz, Schinzel [69]. For a generalization see Noether [27b].

Theorem 4.24 does not shed any light on the highest power of a prime ideal dividing $D_{L/K}$. An upper bound for it was obtained by Hensel [02], who confirmed a conjecture of Dedekind [82] (see Proposition 6.4). See also Bauer [19a], [21b], Ore [25b,c], [26a,d], [27], Yokoi [66].

For Theorem 4.26 and other properties of the differents and discriminants of composite fields see Bauer [21c], Hensel [89], [93], [97d,e], [99], Kataoka [80], Liang [73], Motoda [75], Pumplün [66], Rados [30], Tôyama [55].

The analogue of Corollary 4 to Theorem 4.24 fails for relative extensions, although it holds in certain particular cases. Examples of fields K having no proper unramified extensions were given in Kuroda [62] and Nakahara [73]. Class field theory shows that such fields must have $h^*(K) = 1$, since otherwise there exist Abelian unramified extensions. In fact, the maximal unramified Abelian extension of K has its Galois group isomorphic to $H^*(K)$. For non-Abelian unramified extensions see Elstrodt, Grunewald, Mennicke [85], Hajir, Maire [02], Maire [00], J.H.Smith [69], Taussky [37b], Uchida [70], Y.Yamamoto [70]. Maximal unramified extensions M/K of imaginary quadratic fields with $h = 2$ were determined (for $d(K) = -427$ under GRH) in Yamamura [96].It turned out that M is either the first or the second Hilbert class-field of K. The same task for fields with small conductors was fulfilled in Yamamura[97].

4. The irreducibility of cyclotomic polynomials F_m was for prime m established by Gauss [01] (cf. Kronecker [45a,b], [56b]). The first proof in the general case was given by Kronecker [54]. We presented the proof found by Grandjot [24]. Other proofs may be found in Arndt [58b], Dedekind [57], Landau [29], Lebesgue [59], Levi [31], Schur [29a], Späth [27], Toepken [37]. A survey of early proofs gave Ruthinger [07].

Irreducibility of cyclotomic polynomials in extensions of $\mathbb{Q}$ was considered in Kronecker [54], Nagell [64a], Petersson [55], [59], Pumplün [63], Weisner [28]. For the factorization of $F_m \bmod p$, which can also be obtained from Theorems 4.33 and 4.40, see Ballieu [54], Chowla, Vijayaraghavan [44], Guerrier [68]. For Theorem 4.40 see Bauer [39], Nagell [19], [64a], Rados [06].

5. *Additive Galois-module structure.* Theorem 4.28 is due to E.Noether [32], and the presented proof was found by W.C.Waterhouse [79]. For other proofs see Berger, Reiner [75], Cassels, Wall [50], Chapman [96], Chevalley [33],

Deuring [32], Stauffer [36], Winter [72]. This theorem implies the existence of an element $\omega \in L$ with $L = K[G]\omega$. The possible ω's were studied in Bushnell [77b], [79], [83], Everest [83], Girstmair [96], Halter-Koch, Lorenz [81], Okada [80].

Deuring [32] utilized Theorem 4.28 to deduce the main theorems of Galois theory.

Martinet [69] showed that a normal extension L/K with Galois group G is tame if and only if R_L is a projective $R_K[G]$-module.

For certain large classes of fields tame ramification is sufficient for the existence of a normal integral basis (NIB). This happens, for example, for absolute Abelian fields (the *Hilbert-Speiser theorem*, Hilbert [97], Satz 132, Speiser [16]; see the Corollary to Proposition 8.1). For an algorithm in this case see Schlickewei, Stepanov [93]. The same holds for fields with dihedral Galois group D_n (Miyata [80]; for n being an odd prime: Martinet [69], [71b]; for $n = 2^k$: Fröhlich, Keating, S.Wilson [74] (cf. Cougnard [00]); for $n = p^k$: Taylor [78a]), as well as for all fields of square-free degree (Ph.Cassou-Noguès [77], [78], Taylor [80a], [81a], [82a]). For other classes of fields see Cougnard [72], [73], [74], [80], Fröhlich [74a], [75], [76a], Ichimura [95], [96],[01b], Ichimura, Kawamoto [03], Jaulent [81a], Kawamoto [84], Queyrut [72].

In Gómez Ayala [96] it was shown that if p is an odd prime, $K \subset L \subset \mathbb{Q}(\zeta_p)$, and $[L : K] = 2$, then L/K has a NIB. Necessary and sufficient conditions for the existence of relative normal integral bases in an extension L/K in the case when L has Galois group C_2^n and $[L : K] = 2$ were given in Ji [98]. The case $n = 2$ was earlier treated in Srivastav, Venkataraman [97] (cf. Spearman, Williams [96a]). A criterion in case of Kummer extensions of prime degree appears in Goméz Ayala [94] (cf. Replogle [01]). For normal bases of cyclotomic fields over their subfields see Brinkhuis [83], Cougnard [85], [86], Greither [90].

For a relation between power bases and normal integral bases in unramified cyclic extensions of prime degree see Childs [77], Ichimura [00b], [01a].

For relative NIB see also Itoh [98].

It has been established in Greither, Rubin, Srivastav [99] that $\mathbb{Q}$ is the only algebraic number field such that its every tame Abelian extension has a NIB (cf. Conrad, Replogle [03]). On the other hand, if L/K is Abelian with Galois group G, then R_L is a free $\mathbb{Z}[G]$-module (Taylor [78b]).

The first example of a tame extension of the rationals without a NIB produced Martinet [71a]. His example had the quaternion group H_8 for Galois group. In Martinet [77b] a method is given to produce infinitely many such examples. For other examples see Brinkhuis [81a], Cougnard [83a].

Confirming a conjecture of Serre, Fröhlich [72] proved that if $K/\mathbb{Q}$ is a tame extension with quaternion group H_8, then K has a NIB if and only if the so-called "root-number" $W(\chi)$, corresponding to the unique irreducible symplectic character χ of H_8, equals unity (cf. Fröhlich [76b], Martinet [77b]). This in turn is equivalent to the non-vanishing at $s = 1/2$ of Artin's L-

function corresponding to χ (Armitage [72]). This condition can be also expressed in an elementary way (Fröhlich [72], Martinet [77b]).

Two modules over a ring R are called *stably isomorphic* if with suitable free modules F_1, F_2 one has $M \oplus F_1 \sim N \oplus F_2$. If $\mathfrak{p}$ is a prime ideal of a Dedekind domain R, then denote by $R_\mathfrak{p}$ the closure of R in the corresponding completion of K, the field of quotients of R. Denote by $Cl(R[G])$ the group of classes of stably isomorphic locally free rank one $R[G]$-modules, i.e., finitely generated modules M, whose $\mathfrak{p}$-completions are free $R_\mathfrak{p}[G]$-modules with one free generator. It was proved in Noether [32] that if L/K is normal with Galois group G, then R_L is a locally free $R_K[G]$-module if and only if the extension L/K is tame. Hence for every normal tame extension L/K one can consider the class $[R_L]$ of R_L in $Cl(R_K[G])$. Clearly, $[R_L] = 1$ is necessary for the existence of a NIB, but this condition is, in general, not sufficient. The set of values of $[R_L]$ when L/K runs over tame extensions with a fixed Abelian group was described in McCulloh [87]. The case of an elementary Abelian p-group was treated in McCulloh [83] (cf. Sodaïgui [88]).

The ring R_K is called *stably free* over $\mathbb{Z}[G]$, if $R_K \oplus \mathbb{Z}[G] \sim \mathbb{Z}[G] \oplus \mathbb{Z}[G]$. The first example of a Galois extension $K/\mathbb{Q}$ with stably free R_K, which is not free, was given by Cougnard [94]. In this example the Galois group G is a quaternion group of 32 elements.

Fröhlich conjectured that $[R_L]$ is related to Artin root numbers, appearing in the functional equation of Artin's L-functions associated with the extension L/K, and this has been proved by Taylor [81a] (for a generalization to the wild case see Taylor [95]). His result implies in particular $[R_L]^2 = 1$ and shows that if L/K is a tame normal extension, whose Galois group G does not have any irreducible symplectic[1] characters, then R_L is a free $\mathbb{Z}[G]$-module. The last result applies, in particular, when G is either Abelian, or dihedral, or of odd order, as in these cases there are no symplectic characters. The Abelian case was settled already in Taylor [78b].

A simple criterion for the existence on a NIB in a tame extension of degree 12 with quaternion Galois group was given in Cougnard, Queyrut [02]: the product of primes with ramification index equal to 3 has to be congruent to unity mod 3.

The connections between normal integral bases and Artin root-numbers in the tame case were presented in the book by Fröhlich [83a] (for earlier expositions see Cougnard [83b], Fröhlich [74b], [77a], Martinet [73]).

Chinburg [85] defined three new invariants of normal extensions L/K, which lie in the locally free class group of $\mathbb{Z}[G]$, and stated three conjectures about them. One of these invariants, denoted $\Omega(L/K, 2)$, coincides with $[R_L]$ in the tame case, and the corresponding conjecture states that the analogue of the main theorem of Taylor [81a] holds for $\Omega(L/K, 2)$. This subject was

[1] Recall that a real-valued character χ of G is called *symplectic* if it corresponds to a matrix representation of the form $G \longrightarrow GL_N(\mathbf{H}) \longrightarrow GL_N(\mathbb{C})$, where $\mathbf{H}$ denotes the ring of quaternions.

treated in the book of Snaith [94]. See Burns [95a,b], Burns, Holland [97], Greither [96], [98], Holland [92], [94], Holland, S.M.J.Wilson [94], Hooper, Snaith, van Tran [00], Kim [91], [92], Ritter, A.Weiss [97], Snaith [95a,b] for various results concerning Chinburg's invariants. It follows from them i.a. that all three Chinburg's conjectures are true for real Abelian fields of odd prime conductor.

For the wildly ramified case see also Bergé [78], Cassou-Noguès, Queyrut [82], Cassou-Noguès, Taylor [00], Fröhlich [78], Holland, S.M.J.Wilson [93], Queyrut [81a,b], [82], S.M.J.Wilson [80], [89], [90].

There is another class-group of the group-ring $\mathbb{Z}[G]$ used in this context. Theorem 4.28 shows that if $K/\mathbb{Q}$ is normal with Galois group G, then $K = Q[G]\omega$ holds with a suitable $\omega \in K$, and it follows that there exists an invertible $\mathbb{Z}[G]$-ideal $I \subset \mathbb{Q}[G]$ with $R_K = I\omega$. It is clear that K has a NIB if and only if I is principal. Hence, if we introduce the class-group $cl(\mathbb{Z}[G])$ as the factor group of the group of all invertible fractional $\mathbb{Z}[G]$-ideals contained in $\mathbb{Q}[G]$ by the subgroup of such principal ideals, then K will have a NIB if and only if the image (R_K) of I in $cl(\mathbb{Z}[G])$ equals 1. If for a given group G we put

$$R(G) = \{(R_K) : \ K/\mathbb{Q} \text{ tame }, Gal(K/\mathbb{Q}) = G\},$$

then the question arises how large $R(G)$ can be. The case $G = C_p^n$ (p prime, $n \geq 1$) was settled in McCulloh [82].

On class-groups of group rings the reader is advised to consult Reiner [76] and Taylor [84], and the literature quoted there.

If L/K be a normal extension with Galois group G, then

$$A_{L/K} = \{\alpha \in K[G] : \ \alpha R_L \subset R_L\}$$

is called the *associated order of the extension* L/K. If $K = \mathbb{Q}$ and G is Abelian, then Leopoldt [59] showed that R_K is a free A_K-module, and a simple proof can be found in Lettl [90a]. This remains true for Abelian extensions of cyclotomic fields (Bley [95], Byott, Lettl [96], Chan, Lim [93]), but J.Brinkhuis [87] showed that it may fail for certain other Abelian extensions. Cf. Bergé [72], [78], [81], Cougnard [75], [76], [77], Fröhlich [76b], [77c], Girstmair [92a], Jacobinski [63], Jaulent [81a,b], Leopoldt [59], Martinet [72], Taylor [81b]. Moreover, if $L/\mathbb{Q}$ is Abelian, and $\mathbb{Q} \subset K \subset L$, then it has been shown in Lettl [98] that R_L is locally free over $A_{L/K}$, i.e., the closure of R_L in the completion $L_\mathfrak{p}$ is free over the corresponding associated order for every prime ideal $\mathfrak{p}$ of R_K.

For Galois structure of ideals see Jaulent [81b], Ullom [69], [74a].

In Leopoldt [59], [62] one finds an explicit description of the $\mathbb{Z}[G]$-module R_K as a direct sum of cyclic $Z[G]$-modules in the case of absolute Abelian extensions. This case was also considered in Acciaro, Fieker [00], Bertrandias [79], Chatelain [70], [73], Jakubec, Kostra [92], [98], Ullom [69], Yokoi [60].

Kummerian extensions were treated in Childs [77], [80], [81], Fröhlich [62b], McCulloh [77], Taylor [80b].

M.Newman, O.Taussky [58] and R.C.Thompson [62] described extensions $K/\mathbb{Q}$ which cannot have more than one NIB apart from those obtained by permutations and sign changes. These results can be also deduced from Higman [40].

New necessary conditions for the existence of NIB were found by Brinkhuis [81a,b], [83], [84], who related the Galois structure of R_K to the embedding problem for fields.

For other results concerning the Galois structure of R_K and normal integral bases see Brinkhuis [95], Chinburg [83b], Cougnard [82], Martinet, Payan [67], Maurer [78b], Taylor [82b], [83], Ullom [80], [81], Vostokov [77].

6. Kummer [47b], [56] actually defined ideal prime numbers in a cyclotomic field as formal factors of a rational prime p, imitating the factorization mod p of the corresponding cyclotomic polynomial. This allows us to consider him as the originator of Theorem 4.33, which appeared first in its modern form in Dedekind [78] (cf. Engstrom [30b], Zolotarev [74]). Kronecker [82] related the factorization of primes in extensions of $\mathbb{Q}$ to the factorization mod p of the corresponding norm forms, and this method was also used later in Bauer [19b], Hensel [94a] and Ore [26d].

Ore [23], [25a], [27] employed a method which is p-adic in nature and based on the behaviour of the defining polynomial mod p^N for sufficiently large N (cf. Bauer [36], Bauer, Chebotarev [28]). In Ore [28a] he used an approach based on the study of Newton's polygons, associated with a suitable polynomial. This method was put into a more general context in Montes, Nart [92].

The simple proof of Lemma 4.32 was communicated to the author by Schinzel.

Theorem 4.34 is due to Dedekind [78] (cf. also Hensel [94b], [97b] and Ore [27]). Proposition 4.35 was first proved in Gauss [01].

Proposition 4.36 is due to Żyliński [13], and Nakamura [74] generalized it to relative extensions. Unramified prime divisors of the index $i(K)$ were described in Hensel [84] (cf. Hensel [94b]). See also Carlitz [33], [52], Nagell [66].

The maximal power p^a of a given prime p which can divide $i(K)$ was in certain cases determined in Engstrom [30a]. For $n = 3$, $p = 2$ his result gives $a = 3$ (cf. Spearman, Williams [02b] and Tornheim [55] for the cubic case). Śliwa [82a] determined the exponent a for all unramified primes p. See also Del Corso, Dvornicich [02], Gaál, Pethő, Pohst [91], Nart [85]. Upper and lower bounds for the minimal index of an integer were obtained in Thunder, Wolfskill [96].

It has been shown in Nakahara [87] that for every N there exist cyclic quartic fields K whose all integers have their indices exceeding N, but $i(K) = 1$. The same result for Abelian noncyclic quartic fields was obtained in Nakahara [83].

7. To use Theorems 4.33 and 4.34 one has to factorize polynomials over finite fields. There are several algorithms for this purpose. See the books of Knuth [69], Lidl, Niederreiter [83], McEliece [87] and Shparlinski [92], as well as the survey of von zur Gathen, Panario [01], and the literature quoted there.

8. The proof of Theorem 4.37 presented here is due to T.Nagell. An analytical proof will be given in Chap. 7. Other proofs, some of which apply also to more general situations, can be found in Dress [64], Dujčev [56], Moriya [50], Nagata, Nakayama, Tuzuku [53], Voloch [00]. A counterpart to Theorem 4.37 is also true: there exist infinitely many prime ideals which do not split completely in a given extension (see Corollary 5 to Proposition 7.16).

Class-field theory determines the prime ideals splitting in an Abelian extension L/K as those whose classes lie in a certain subgroup of $H_I^*(K)$ with a suitable I. This property characterizes Abelian extensions (see e.g. Cassels, Fröhlich [67]. Cf. Gauthier [78]). Bruckner [66] described absolute normal extensions in which the splitting primes are exactly those which are representable by binary quadratic forms from a given set.

Hasse [26a,b] proved that for any algebraic number field K there are infinitely many extensions L/K of a fixed degree in which prime ideals from a given finite set factor in a prescribed way, subject only to conditions resulting from Theorem 4.5 (cf. Ore [26c]).

9. Theorem 4.39 for the field $\mathbb{Q}(i)$ was known already to Gauss [32]. In this case, as for all other fields with class-number 1, prime ideals correspond to classes of irreducible integers, and their description can be carried out in elementary way (see e.g. Hardy, Wright [60, Chap.XII). An analogue of Theorem 4.39 for relative quadratic extensions is given in Hilbert [99].

Theorem 4.40 goes back to Kummer [47b], [56] (see also Bachman [66], Bhaskaran [71]). Also Theorem 4.42 was proved by Kummer [59] in a special case. The general case is essentially due to Hilbert [99, Satz 149]. Cf. Hensel [18], [21a], Rella [24a].

Factorizations in cubic fields were considered in Agou [71], Dedekind [00], Hasse [30b], Latimer [29], Llorente, Nart [83], Martinet, Payan [67], Reichardt [33], Wahlin [22], Westlund [13].

The case of normal fields with Galois group C_2^n was considered in Zhang X. [82].

Factorizations in Abelian extensions are described by class-field theory, but in the case of the rational base-field this can be done in an elementary way, which will be presented in Chap. 8.

There is no comparable approach in the non-Abelian case and our knowledge is reduced to extensions of a rather special form. On this topic see Bruckner [68], Büsser [44], Fröhlich [60a], Furuta [59], [61], [77], Gut [32], [33], Halter-Koch [71b], Ito [77], S.Kuroda [51], S.-N.Kuroda [70], Mann, Vélez [76], Sato [81], Vélez [77], [78], van der Waall [74a]. A connection with

the theory of modular forms was established by Shimura [66]. See Chowla, Cowles [77], Hiramatsu [82].

Relations between factorizations in two extensions and their composite were studied in Bauer [16b], [20], [21a], [40a,b], Hensel [89], Herbrand [31a], Maus [67], Ore [26b], Vassiliou [32].

In Maurer [73] it has been shown that the factorization of a rational prime in an extension is determined by the properties of trace form

$$F(X_1, \ldots, X_n) = \det \left[Tr_{K/Q}(\omega_i \omega_j) \right]_{i,j},$$

where $\omega_1, \ldots, \omega_n$ is an integral basis of K.

For other questions concerning factorizations of prime ideals in extensions see Barrucand, Laubie [82], Bhaskaran [74], Hasse [51c], MacCluer [71], Parry [71a,b,c], Reichardt, Wegner [37].

A rational prime which splits completely in K, but remains irreducible is called a *sci prime*. Such primes were described for biquadratic fields in McCoy, Parry [01].

10. Proposition 4.44 is very old. A proof of it without using ideal theory was given by Lánczi [65] (cf. Zaupper [83]). Elementary proofs in special cases may be found in Gauss [32], Rudin [61]. For the converse of this result see Theorem 8.29.

The knowledge of prime ideals having small norms suffices, in principle, for the determination of the class-number and the structure of the the class-group. Algorithms for that purpose are described in H.Cohen [93] and Pohst [93]. A rather quick algorithm (which is subexponential under *GRH*) was found by Buchmann [90]. In the case of Abelian fields the class-number can be expressed in terms of values of Dirichlet L-functions $L(s.\chi)$ at $s = 1$ (see Theorem 8.10).

11. The argument used in the proof of Theorem 4.47 was utilized by Hecke [18,II] in the definition of his ideal numbers, which he utilized for the construction of a certain class of zeta-functions, called now *Hecke's zeta-functions*. After the invention of ideles and adeles the ideal numbers slowly disappeared.

Proposition 4.49 is due to Furtwängler [08], and has been rediscovered several times. Proposition 4.25 appears in Yokoi [68b] and Yokoyama [65]. Other results on these topics may be found in Chevalley [31], Dénes [52a], Draxl [70], Fröhlich [52], Iwasawa [55a], Ohta [78], Okamoto [76], W.Scharlau [73], Schipper [77], Yokoi [67], Yokoyama [65].

12. The structure of the class-group of a normal extension $K/\mathbb{Q}$ as a Galois module remains still largely unknown. One of the central problems here is the determination of the ideal of relations of $H(K)$ in $\mathbb{Z}[G]$, i.e., the set of all elements $\sum a_g g \in \mathbb{Z}[G]$ such that for every class $X \in H(K)$ one has

$$\prod_{g \in G} g(X)^{a_g} = 1.$$

It follows from Propositions 4.7 (i) and 4.8 that this ideal always contains $N = \sum_g g$, and in the case of an imaginary Abelian extension other non-trivial relations are provided by the *Stickelberger ideal*

$$S = \mathbb{Z}[G] \cap A\mathbb{Q}[G],$$

with $A = f^{-1} \sum_a a g_a^{-1}$, where f is the *conductor* of K, i.e., the smallest integer with $K \subset \mathbb{Q}(\zeta_f)$ (which exists by the Kronecker-Weber theorem; see Theorem 6.18) and g_a is the restriction to K of the automorphism of $\mathbb{Q}(\zeta_f)$, given by $\zeta_f \mapsto \zeta_f^a$. The fact that S annihilates $H(K)$ was established for cyclotomic fields by Stickelberger [90] (in the case $K = \mathbb{Q}(\zeta_p)$ this is an immediate consequence of a result in Kummer [47b]; see Hilbert [97, Satz 136]). For other proofs see Childs [81], Fröhlich [77b]. For the general case see Coates [77], S.Lang [78] and Washington [82], where further references can be found.

Let K be a normal complex field with Galois G, let $s \in G$ act as the complex conjugation, put for any $\mathbb{Z}[G]$-module M

$$M^- = \{a \in M : \ s(a) = -a\},$$

and let S be the Stickelberger ideal. Iwasawa [62] showed that if $K = \mathbb{Q}(\zeta_p)$ with prime p, then the index of S^- in $\mathbb{Z}[G]^-$ equals $h(K)/h(K^+)$ (see Skula [81] for another proof). This result was extended by Sinnott [78] to arbitrary cyclotomic fields, and C.G.Schmidt [79], Sinnott [80] and Iimura [81b] did the same for arbitrary complex Abelian fields. See also Kimura,, Horie [82], [87]. For further generalizations consult Cassou-Noguès, Taylor [91], Bayad, Bley, Cassou-Noguès [96].

An analogue of the Stickelberger ideal annihilating $H_I^*(K)$ was constructed by C.G.Schmidt [82] for cyclotomic K. For other results of annihilators of the class-group see G.Gras [79a,b], Kobayashi [82], Oriat [81].

The action of the Galois group on $H(K)$ was studied also in Cornell, Rosen [81], Dénes [52a], Gerth [75c], Iwasawa [66], Komatsu, Nakano [01], S.N.Kuroda [64b] and Lemmermeyer [03].

The group $Am(L/K)$ was studied in the case of cyclic extensions of prime degree in G.Gras [72b], [73], [74a], [78], Moriya [30]. A formula for the number of elements of ray class-groups and their epimorphic images, which are invariant under the action of the Galois group was given by G.Gras [94].

For other classes of fields see Furuya [82], Jaulent [81c], Payan [73].

The maximal factor group of $H(K)$ on which the Galois group operates trivially is called the *central ideal class group of* K. It has been studied in Fröhlich [54a], [83b], Furuta [71], [76], [77], Garbanati [78a], Shirai [75], [78], [79].

13. The class-field theory provides a canonical extension of K having the property stated in Theorem 4.47, namely the *Hilbert class field* $\bar{K}$ of K, defined as the maximal Abelian unramified (also at infinity) extension of K. The proof of his property for $\bar{K}$ has been reduced by Artin [30a] to a group-theoretical statement, proved later by Furtwängler [30] (*Principal Ideal Theorem*, *Hauptidealsatz*). Other proofs can be found in Borevich [57], Iyanaga [34], Magnus [34], Schumann [37], Taketa [32]. For various generalizations and analogues see Furuya [77], Herbrand [32c], Iyanaga [31], [39], Kempfert [62], Kuniyoshi, Takahashi [53], Miyake [80a], Takahashi [64], [65], Tannaka [33a,b], [34], [49], [50], [56], [58], Tannaka, Terada [49], Taussky [32], Terada [50], [52], [53], [54a,b], [55], [71], Zink [75].

If a class $X \in H(K)$ lies in the kernel of $i^*_{L/K}$, then X is said to *capitulate in* L. Thus the Principal Ideal Theorem asserts that all classes capitulate in $\bar{K}$. The first result concerning capitulation is the Theorem 94 of Hilbert [97], stating that if L/K is cyclic and unramified of degree N, then the order of the kernel of $i^*_{L/K}$ divides N (cf. Taussky [69], [71].

Capitulation in various classes of fields was considered in Azizi [97], [00], Azizi, Mouhib [03], Benjamin, Sanborn, Snyder [94], Bond [81], Chang [77], Chang, Foote [80], Cremona, Odoni [90], Furuya [77], Gerth [93], G.Gras [97], Heider [84], Heider, Schmithals [82], Iwasawa [89], Jehne [77a], Kisilevsky [70], Schmithals [85], Scholz, Taussky [34], Terada [71].

It has been conjectured for a long time that if L/K is an Abelian unramified (also at infinity) extension, then at least $[L : K]$ classes capitulate in L. This assertion, which generalizes both Hilbert's Theorem 94 and the Principal Ideal Theorem, has been proved by Suzuki[91]. A further generalization was obtained by Gruenberg and A.Weiss [00]).

Surveys of the capitulation problem were given in Jaulent [88] and Miyake [89].

14. If $h(\bar{K}) \neq 1$, then one can consider the Hilbert class-field of $\bar{K}$ and continue this process. It has been conjectured (see Hasse [26c]) that this process terminates, and that in this way one will be led to an extension L/K with $h(L) = 1$ (the *class-field-tower problem*, *Klassenkörperturmproblem*). It turned out, however, that the class-field tower may be infinite (Golod, Shafarevich [64]). This happens, e.g., if K is a quadratic field with sufficiently many ramified primes. Previously Scholz [29] noted that this tower may be arbitrarily long. For expositions of the Golod-Shafarevich theorem see Panella [66], Roquette [67], Serre [66]. Cf. Koch [69], [75], Kostrikin [65], Vinberg [65]. It was shown in Kuzmin [69] that if $K/\mathbb{Q}$ is normal and has at least 8 ramified primes, then its class-field tower is infinite. Examples of quadratic fields with an infinite class-field tower and few ramified primes were given in Martinet [78], Matsumura [77] and Schmithals [80a] (see also Gerth [03]). It was shown in Schoof [86] that there are infinitely many real and imaginary quadratic fields with two ramified primes and infinite class-field tower (cf. Hajir [96], Schmithals [80a]). Cubic fields were considered in Maire [97], [98].

For study of the first few layers of the class-field tower of quadratic fields see Benjamin [93], [99], Benjamin, Lemmermeyer, Snyder [97], [98a,b], Benjamin, Snyder [95], Brink, Gold [87], Gerth [98], Hajir [97b], Kisilevsky [76], Lemmermeyer [94a], [97a], Taussky [37a].

Class-field towers of other classes of fields were studied in Browkin [63], Brumer [65], Cornell [83a,b], Furuta [72], Lamprecht [67], Scholz, Taussky [34], Shafarevich [63b], T.Takeuchi [79], [80], E.Yoshida [03]. The growth of the p-class group in layers of a p-class-field tower was studied in Hajir [97a]).

15. The *ray class-fields* mod I of a given field K are defined as the maximal Abelian extensions of K in which only primes ideals dividing a given ideal I are ramified. The Galois group of such a ray class-field equals $H_I(K)$ if no ramification at infinity is allowed, and equals $H_I^*(K)$ otherwise. For imaginary quadratic fields the ray class-field are described by the classical theory of complex multiplication, which goes back to H.Weber ([96b,III], [97]) and Fueter [07], [11], and which assumed its modern form in Hasse [27] and Deuring [49], [52]. For an introduction to complex multiplication see Borel *et al.* [66]. The paper of Hasse [27] gives a pair of generators for every such field, and Ramachandra [64] succeeded in giving in each case one generator, which is the value at a point of K of a holomorphic function, independent of K. This is an analogue of the case $K = \mathbb{Q}$, where the Kronecker-Weber theorem (see Theorem 6.18) shows that the ray-class field mod $m\mathbb{Z}$ is equal to the m-th cyclotomic field.

A generalization of the classical theory of complex multiplication, leading to the construction of class-fields for a large class of fields, was developed by Shimura and Taniyama [61]. See also Shimura [62], [68], [71a,b], [72].

For algorithms and/or explicit determination of class-fields see the book of H.Cohn [85], as well as the following papers: Barrucand, H.Cohn [73], H.Cohen, Diaz y Diaz, Olivier [98a], H.Cohn [79a,b], [81a,b], [83], H.Cohn, Cooke [76], Daberkow, Pohst [98], Eichler [56], Fieker [01], Gogia, Luthar [78], G.Gras [72c], Gut [43a,b], Hasse [33], [64], Hasse, Liang [69], Hecke [12], [13], Herz [66], Hilbert [99], Kaplan [77a], Liang, Zassenhaus [69], Madden, Vélez [80], Schertz [78a].

One of the main problems of algebraic number theory is the construction of an analogue of the class-field theory for non-Abelian extensions. An early attempt to do this was made by Krasner [47]. A way towards its solution is the *Langlands program*, which predicts deep connections between number theory and group representations. An introduction to it was given in Gelbart [84] and Murty [93]. Its analogue for p-adic fields has been established in Harris, Taylor [01] and Henniart [00] (cf. Bushnell, Henniart [01]), and for local fields of positive characteristic in Laumon, Rapoport, Stuhler [93] (for expositions see Carayol [00], M.R.Murty [02], Rogawski [00]).

16. It has been proved in Cassou-Nogues, Taylor [87a,b], [88], Cougnard [90], Cougnard, Fleckinger [89], Gómez Ayala [94], [95], Schertz [89], [91] that

many extensions L/K, where $K \subset L$ are ray class-fields of an imaginary quadratic field, have relative power integral bases. This does not happen always, as suitable examples show (Cougnard, Fleckinger [89]). Even in the simplest case, when K is an imaginary quadratic fields with $h = 1$, such examples were given in Cougnard, Verant [92] and Gómez Ayala, Schertz [93]. Cf. Greither [97], Kawamoto [01], Komatsu [97].

17. The use of cohomology in algebraic number theory was initiated by Hochschild and Nakayama [52] and Nakayama [52]. This approach turned out to be very successful in restating the class-field theory in a purely algebraic fashion. For an introduction to the application of cohomological algebra to algebraic number fields see Neukirch, Wingberg [00], where one can find further literature.

18. Several authors devoted their attention to maximal extensions with prescribed properties of number fields. Denote by $\hat{K}$ the algebraic closure, and by $\hat{K}^{ab}$ the maximal Abelian extension of an algebraic number field K. Kubota [57] determined Ulm's invariants of $Gal(\hat{K}^{ab}/K)$, and a study of Galois groups of maximal p-extensions of algebraic number fields makes the contents of the book of Koch [70]. Maximal solvable extension K^{sol} of an algebraic number field K was studied by Iwasawa [53b], who proved that the group $Gal(K^{sol}/K^{ab})$ does not depend on K.

It has been shown by Neukirch [69a] that if K, L are finite normal extensions of the rationals with $Gal(\hat{K}/K) \sim Gal(\hat{L}/L)$, then $K = L$. The analogue of this result for maximal Abelian extensions is not true (Onabe [76]). The conjecture of Neukirch [69b] that $Gal(\hat{Q}/Q)$ has only inner automorphisms has been proved by Ikeda [75b], [77] and Uchida [76a], [77a]. A simpler proof appears in Neukirch [77] (see also Ikeda [75a], Kanno [73], Komatsu [74]). For a survey of results concerning $Gal(\hat{Q}/Q)$ see Geyer [78] and Neukirch [74a].

EXERCISES

1. Prove that if L/K is normal, then the kernel of the trace map $L \longrightarrow K$ equals the additive group generated by the set $\{(1-\sigma)a : \sigma \in Gal(L/K), a \in L\}$.

2. Show that every normal extension of an odd degree is unramified at infinity and prove that one cannot remove the assumption of normality.

3. Let K be a quadratic field and let $a \in R_K$. For $A = \mathbb{Z}[a]$ determine its conductor and A^*.

4. Compute the different of a pure cubic extension of the rationals.

5. Prove the analogue of Theorem 4.28 for a finite field K.

6. (McCulloh) Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(i)$. Prove that L/K has a relative integral basis, but it does not have a normal integral basis.

7. (i) Let $K/\mathbb{Q}$ be normal with Galois group G, let $\omega \in R_K$, and assume that the set $\{\sigma(\omega) : \sigma \in G\}$ forms a normal integral basis of K. Prove that there exists

$\omega' \in R_K$, not of the form $\pm\sigma(\omega)$ with $\sigma \in G$, such that its conjugates form a normal integral basis if and only if the group ring $\mathbb{Z}[G]$ has invertible elements not of the form $\pm\sigma$ ($\sigma \in G$).

(ii) (Newman, Taussky [58]) Prove that if, moreover, G is cyclic of order 2, 3, 4 or 6, then K can have at most one normal integral basis, up to permutations and sign changes.

(iii) Show on an example that (ii) may fail if G is cyclic of order 5 or 8.

8. Determine the factorization of ramified primes in pure cubic fields.

9. Prove that in a cubic field K one has $i(K) > 1$ if and only if 2 splits completely in $K/\mathbb{Q}$.

10. Let $K/\mathbb{Q}$ be normal of degree 4 with a non-cyclic Galois group. Prove that with suitable $a, b \in \mathbb{Z}$ one has $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, determine the discriminant $d(K)$, and find the law of decomposition of prime ideals in $K/\mathbb{Q}$.

11. Let K be a quadratic field and put $D = |d(K)|$. Prove the inequality

$$h(K) < \frac{1}{3}\sqrt{D}\log D$$

for all real K and for all complex K with sufficiently large D.

5. $\mathfrak{p}$-adic Fields

5.1. Principal Properties

1. In this chapter we shall consider fields which are completions of algebraic number fields under discrete valuations. According to Theorem 3.1 every valuation gives rise to a complete field, uniquely determined up to a topological isomorphism. By Theorem 3.3 every discrete valuation v of an algebraic number field K is induced by a prime ideal $\mathfrak{p}$ of its ring of integers. The completion of K under v will be denoted by $K_\mathfrak{p}$ or K_v and called the *$\mathfrak{p}$-adic field*. In the case of $K = \mathbb{Q}$ we shall not distinguish between the prime p and the prime ideal generated by it, and we shall write $\mathbb{Q}_p$ for the field which is the completion of $\mathbb{Q}$ under the valuation induced by $p\mathbb{Z}$. The field $\mathbb{Q}_p$ is called the *p-adic field*.

It is not aim to present the full story of $\mathfrak{p}$-adic fields, and we shall develop their theory only to such extent as needed for our immediate purposes. The interested reader should consult the books of Cassels [86], Fesenko, Vostokov [93], Gouvêa [93], Koblitz [77], Mahler [73], Robert [00] and Serre [62] for more information.

First we define the integers and units of a $\mathfrak{p}$-adic field. Let K be an algebraic number field, $\mathfrak{p}$ a prime ideal of R_K, v the valuation of K associated with $\mathfrak{p}$, $K_\mathfrak{p}$ the completion of K under v and k the quotient field $R_K/\mathfrak{p}$. The extension of v to $K_\mathfrak{p}$ will be denoted by the same letter v. By Corollary 1 to Theorem 3.1 we see that v is discrete, the ring $R_\mathfrak{p} = \{x \in K_\mathfrak{p} : \ v(x) \leq 1\}$ is the closure of the ring $R = \{x \in K : \ v(x) \leq 1\}$, and $\mathfrak{P} = \{x \in K_\mathfrak{p} : \ v(x) < 1\} = \mathfrak{p}R_\mathfrak{p}$ is a prime ideal of $R_\mathfrak{p}$, which is the closure of the prime ideal $\{x \in K : \ v(x) < 1\}$ of R. The proof of Theorem 3.1 shows moreover that the sets $v(K)$ and $v(K_\mathfrak{p})$ coincide. This enables us to define an extension to $K_\mathfrak{p}$ of the exponent of K corresponding to $\mathfrak{p}$ by putting $\nu(x) = \log_a v(x)$ for non-zero x in $K_\mathfrak{p}$, where the number a from $(0, 1)$ is so chosen that for every non-zero $x \in K$ one has $v(x) = a^{\nu(x)}$. It is convenient also to put $\nu(0) = \infty$.

The ring $R_\mathfrak{p}$ will be called the *ring of integers of* $K_\mathfrak{p}$, and its elements the *integers* of $K_\mathfrak{p}$. For the ring of integers of the p-adic field $\mathbb{Q}_p$ we shall also write $\mathbb{Z}_p$. The invertible elements of $R_\mathfrak{p}$ form a group $U(K_\mathfrak{p})$, which is the *group of units* of $K_\mathfrak{p}$. Clearly an element $x \in K_\mathfrak{p}$ is a unit if and only if one has $v(x) = 1$, i.e., $\nu(x) = 0$.

Proposition 5.1. *(i) The ring $R_\mathfrak{p}$ is a Dedekind domain with trivial class-group, $\mathfrak{P}$ is its unique non-zero prime ideal, and the quotient fields $R_\mathfrak{p}/\mathfrak{P}$ and $R_K/\mathfrak{p}$ are isomorphic.*

(ii) One has $U(K_\mathfrak{p}) = R_\mathfrak{p} \setminus \mathfrak{P}$, and if π is any fixed element of $\mathfrak{P} \setminus \mathfrak{P}^2$, then every non-zero element $x \in K_\mathfrak{p}$ can be uniquely written in the form $x = a\pi^m$ with $a \in U(K_\mathfrak{p})$ and $m \in \mathbb{Z}$. In that case one has $m = \nu(x)$.

(iii) The ring $R_\mathfrak{p}$ is the closure of R_K in $K_\mathfrak{p}$, and, more generally, $\mathfrak{P}^m$ is the closure of $\mathfrak{p}^m$ for $m = 1, 2, \ldots$. One has moreover $\mathfrak{P}^m \cap R_K = \mathfrak{p}^m$.

Proof: Part (i) results immediately from Theorem 1.26, Proposition 1.27 and Corollary 2 to Theorem 3.3, and the first assertion of (ii) follows from (i) and the observation that if a domain has only one non-zero prime ideal, then this ideal consists of all non-invertible elements. To prove the second assertion of (ii) it suffices to remark that if $m = \nu(x)$, then $\nu(x\pi^{-m}) = 0$, and $x\pi^{-m}$ is a unit.

Finally, to prove (iii) observe that (ii) implies the equality $\mathfrak{P}^m = \{x \in K_\mathfrak{p} : \nu(x) = m\}$. □

An explicit form for elements of $K_\mathfrak{p}$ is provided by the following theorem:

Theorem 5.2. *Let K be a field of zero characteristic, complete under a discrete valuation. Denote by R its valuation ring, by P the unique prime ideal of R, and assume that the residue class field R/P is finite. Let A be a system of representatives of R mod P, containing the zero element, and let t_n $(n = 0, \pm 1, \ldots)$ be a sequence of elements of R such that $t_0 \notin P$ and $t_{n+1}/t_n \in P \setminus P^2$ for $n = 0, 1, \ldots$. Then every non-zero element $x \in K$ can be uniquely represented as the sum of a convergent series*

$$x = a_N t_N + a_{N+1} t_{N+1} + \cdots \tag{5.1}$$

with a suitable $N \in \mathbb{Z}$, $a_N, a_{N+1}, \ldots \in A$ and $a_N \neq 0$.

Proof: Assume first that x is a non-zero element of R. Since $t_0 \notin P$ we may choose $a_0 \in A$ so that $x \equiv a_0 t_0 \pmod{P}$. Then $x_1 = (x - a_0 t_0)/t_1$ lies in R. Choose in turn $a_1 \in A$ with $a_1 \equiv x_1 \pmod{P}$, and put $x_2 = (x_1 - a_1)t_1/t_2 \in R$. If the elements x_i and a_i are already chosen for all $i \leq r$ and satisfy $x_i \equiv a_i \pmod{P}$, then we put $x_{r+1} = (x_r - a_r)t_r/t_{r+1} \in R$, and define $a_{r+1} \in A$ by $x_{r+1} \equiv a_{r+1} \pmod{P}$. Observe now that for every r we have

$$x \equiv a_0 t_0 + a_1 t_1 + \cdots + a_r t_r \pmod{P^{r+1}},$$

hence the series (5.1) converges to x.

If x is an arbitrary non-zero element of K, then write $x = \epsilon t_m$ with a suitably chosen m and a unit ϵ of R. Applying the preceding argument to the element ϵ and the sequence $t'_n = t_{m+n}/t_m$, we obtain (5.1) for our element x.

To prove uniqueness of the representation (5.1) it suffices to show that if we have $c_m t_m + c_{m+1} t_{m+1} + \cdots = 0$, and the elements $c_j \in R$ are either zero or lie outside P, then one has $c_j = 0$ for all j. Assuming $c_m \neq 0$ and dividing by t_m we obtain

$$0 = c_m + c_{m+1} t_{m+1}/t_m + \cdots,$$

and it remains to note that in this series all terms except possibly the first lie in P, thus $c_m \in P$ and $c_m = 0$, contrary to our assumption. □

This theorem permits to extend the assertion of Proposition 5.1 (i):

Corollary 1. *If $\mathfrak{p}$ is a prime ideal in R_K, and $\overline{\mathfrak{p}}$ is the prime ideal of $R_{\mathfrak{p}}$, then for $N = 1, 2, \ldots$ the factor-rings $R_K/\mathfrak{p}^N$ and $R_{\mathfrak{p}}/\overline{\mathfrak{p}}^N$ are isomorphic.*

Proof : For $N = 1$ this is contained in Proposition 5.1 (i). The injection $R_K \longrightarrow R_{\mathfrak{p}}$ maps $\mathfrak{p}^N$ into $\overline{\mathfrak{p}}^N$, hence induces an injective homomorphism of $R_K/\mathfrak{p}^N$ into $R_{\mathfrak{p}}/\overline{\mathfrak{p}}^N$. To prove that it is surjective observe that Proposition 5.1 (i) shows that the elements t_j in (5.1) may be taken from R_K, and this implies that every residue class mod $\overline{\mathfrak{p}}^N$ contains elements from R_K. □

Corollary 2. *For every prime p one has*

$$\mathbb{Z}_p \sim \lim \operatorname{inv} \mathbb{Z}_p/p^m\mathbb{Z}_p \sim \lim \operatorname{inv} \mathbb{Z}/p^m\mathbb{Z},$$

the mappings $R/p^m R \longrightarrow R/p^k R$ being defined for $m > k$, and $R = \mathbb{Z}$, $\mathbb{Z}_p$ by $x \bmod p^m R \mapsto x \bmod p^k R$,

Proof : The first isomorphism follows from the theorem, and the second is a consequence of Corollary 1. □

The problem of convergence criteria for series in $K_{\mathfrak{p}}$ is solved easily by the following proposition:

Proposition 5.3. *If L is a field complete under a non-Archimedean valuation v, then the series $\sum_{n=1}^{\infty} a_n$ ($a_n \in L$) converges if and only if one has $\lim_{n\to\infty} a_n = 0$.*

Proof : The necessity being obvious, we turn to the sufficiency. Assume thus that the sequence $\{a_n\}$ converges to zero, i.e. $\lim_{n\to\infty} v(a_n) = 0$. Then for any $M \leq N$ we have

$$v(a_M + a_{M+1} + \cdots + a_N) \leq \max_{M \leq i \leq N} v(a_i),$$

and the right-hand side tends to zero when M tends to infinity. Therefore the sequence of partial sums of our series is fundamental, hence convergent by completeness of L. □

Now we describe the main topological properties of fields K, satisfying the assumptions of Theorem 5.2.

Theorem 5.4. *The additive and multiplicative groups of K are locally compact topological groups, and the ring R and its ideals P^m $(m = 1, 2, \ldots)$ are compact and open. These ideals form a basis of neighbourhoods of the zero element, and thus R is a totally disconnected topological space.*

Proof : We need a lemma:

Lemma 5.5. *If for $j = 1, 2, \ldots$ we define a ring homomorphism f_j from R/P^{1+j} to R/P^j by*

$$f_j : \ x \mapsto x \bmod P^j,$$

then the inverse limit

$$X = \lim \operatorname{inv} R/P^j$$

is topologically isomorphic with R.

Proof : Let $x \in R$, and let x_j be the image of x in R/P^j under the residue class map. We define a map of R into X by putting

$$f : \ x \mapsto [x_1, x_2, \ldots].$$

It is obvious that f is a ring homomorphism with trivial kernel. Moreover, if $\alpha = [a_1, a_2, \ldots] \in X$ then for any $r \geq 1$ and $m, n \geq r$ we have

$$a_m \equiv a_n \,(\bmod\ P^r).$$

Thus, if we consider a sequence $A_1, A_2, \ldots$ of elements of R with $A_n \bmod P^n = a_n$, then this sequence is fundamental, and for its limit A we have $f(A) = \alpha$. Thus f is surjective, and so it is an isomorphism. It remains to show that both f and its inverse map are continuous, and since these maps are homomorphisms and the underlying space is homogeneous, being a carrier of a topological group, it suffices to show continuity at 0. If a sequence $\{c_n\}$ in R converges to 0, then for every N one has $c_n \in P^N$ for sufficiently large n, hence $f(c_n)$ is of the form $[0, \ldots, 0, x_{N+1}, \ldots]$, thus tends to zero. Conversely, if $y_n = [c_1^{(n)}, c_2^{(n)}, \ldots]$ tends to zero, then for every N and sufficiently large n we have $c_i^{(n)} = 0$ for $i = 1, 2, \ldots, N$. It follows that if $f(x_n) = y_n$, then x_n tends to 0. □

To prove the theorem observe that R is compact as the inverse limit of finite sets, and so are the ideals P^m, as closed subsets of R. Moreover if $a \in P^m$ and $a - b \in P^{m+1}$, then the element b also lies in P^m, showing that P^m is open. The set P is a compact neighbourhood of the zero element in the additive group of K, and $1 + P$ has the same property in the multiplicative

group, whence these groups are locally compact. The remaining assertions are now evident. □

Corollary. *Let $F_1(X_1, \dots, X_r), \dots, F_k(X_1, \dots, X_r)$ be polynomials with coefficients in R. The system of equations*

$$F_i(x_1, \dots, x_r) = 0 \quad (i = 1, 2, \dots, k) \tag{5.2}$$

has a solution in R if and only if for every $m \geq 1$ the system of congruences

$$F_i(x_1, \dots, x_r) \equiv 0 \pmod{P^m} \quad (i = 1, 2, \dots, k) \tag{5.3}$$

is solvable in R.

If for every $m \geq 1$ the system (5.3) has a solution with some $x_i \notin P$, then the system (5.2) has a solution with not all x_i's being zero.

Proof : The necessity is obvious. To prove the sufficiency, let for $m = 1, 2, \dots$ the elements $x_1^{(m)}, \dots, x_r^{(m)} \in R$ form a solution of (5.3). As R is a compact metric space, we can find a sequence m_k such that the sequences $\{x_i^{(m_k)}\}$ are convergent to $y_i \in R$, say. It is clear that the y_i's form a solution of (5.2), and if for some i we have $x_i^{(m_k)} \notin P$, then the same applies to y_i, because P is open. □

2. In this subsection let K be a $\mathfrak{p}$-adic field, R its ring of integers, $\mathfrak{p} = \pi R$ the prime ideal of R, and $k = R/\mathfrak{p}$. For $x \in R$ put $\overline{x} = x \bmod \mathfrak{p} \in k$. Similarly, for every polynomial $W \in R[X]$ we shall denote by $\overline{W}$ the polynomial over k obtained from W be replacing each of its coefficients by its residue in k.

One of the main tools used in the study of $\mathfrak{p}$-adic fields is the theorem, commonly known as *Hensel's lemma*, which we are now going to prove.

Theorem 5.6. *Let W be a polynomial over R. If the polynomial $\overline{W}$ can be written as a product of two relatively prime non-constant polynomials $f, g \in k[X]$, then there exist two relatively prime polynomials $F, G \in R[X]$ satisfying*

$$\deg F = \deg f, \ \overline{F} = f, \ \overline{G} = g, \ W = F \cdot G.$$

If moreover f is monic, then one can also choose a monic polynomial F.

Proof : Let $m = \deg f$, $n = \deg g$. We shall define inductively two sequences, f_k and g_k, of polynomials over R enjoying the following properties:

(a) $\deg f_k = m$, $\deg g_k = n$,

(b) All coefficients of the polynomial $W - f_k g_k$ lie in $\mathfrak{p}^{k+1}$,

(c) All coefficients of the polynomials $f_k - f_{k-1}$ and $g_k - g_{k-1}$ lie in $\mathfrak{p}^k$,

(d) If f is monic, so is f_k.

(e) $\overline{f_0} = f$, $\overline{g_0} = g$.

The existence of such sequences will immediately imply the theorem. In fact, the conditions (b) and (c) show that the coefficients of f_k and g_k form converging sequences, and by (a) the polynomials f_k and g_k converge to certain polynomials F and G, respectively, in the topology defined in the set Ω_N of polynomials over R with degrees not exceeding $N = \max\{m, n\}$ by the family $H + \mathfrak{p}^k R[X] \cap \Omega_N$ with $H \in \Omega_N$ and $k = 1, 2, \ldots$. From (b) follows the equality $W = FG$, (c) and (e) imply $\overline{F} = f$, $\overline{G} = g$, and since f and g are relatively prime, so are F and G. Moreover, if f is monic, then by (d) F is also monic.

So let us now construct the required sequences. Let $f_0 \in R[X]$ be any polynomial of degree m for which $\overline{f_0} = f$, and which is monic, if f is such. Similarly, let $g_0 \in R[X]$ be of degree n with $\overline{g_0} = g$. Assume now that we have already chosen $f_0, g_0, \ldots, f_N, g_N$ subject to (a) - (e) for certain $N \geq 0$. The condition (b) implies that the polynomial $c_N = (W - f_N g_N)\pi^{-N-1}$ has its coefficients in R and since f, g are relatively prime there exist polynomials a_N and b_N over R with $\deg a_N \leq m - 1$ and $\deg b_N \leq n$, satisfying

$$-\overline{c_N} + \overline{a_N} g + \overline{b_N} f = 0,$$

i.e.,

$$-c_N + a_N G + b_N F \equiv 0 \pmod{\mathfrak{p}}.$$

It remains to observe that the polynomials

$$f_{N+1} = f_N + a_N \pi^{N+1}, \quad g_{N+1} = g_N + b_N \pi^{N+1}$$

satisfy (a) - (c) and (e), and if f was monic, also (d). □

Corollary 1. *If W is a polynomial over R such that the polynomial $\overline{W}$ has a simple zero $u \in k$, then there exists an element $a \in R$ such that $W(a) = 0$ and $\overline{a} = u$.*

Proof : Write $\overline{W}(X) = (X - u)V(X)$ with $V \in k[X]$. Since $V(u) \neq 0$, the polynomials $X - u$ and V are relatively prime, thus the theorem shows the existence of a factorization $W(X) = (X - a)U(X)$ with a certain $U \in R[X]$ and $\overline{a} = u$. □

Corollary 2. *If the field k has q elements, then in every non-zero residue class of R mod $\mathfrak{p}$ there is a root of unity of order $q - 1$.*

Proof : Consider the polynomial $f = X^{q-1} - 1$. Every non-zero element of the field k is a root of f, hence it has $q - 1$ distinct roots, and the preceding corollary is applicable. □

Corollary 3. *If p is an odd rational prime and m is a rational integer, not divisible by p, then the field $\mathbb{Q}_p$ contains square roots of m if and only if m is a quadratic residue mod p.*

Proof : Apply Corollary 1 to the polynomial $X^2 - m$. □

Corollary 4. *If $W \in R[X]$ is irreducible over K, then $\overline{W}$ is a power of a polynomial irreducible over k.*

Proof : Otherwise $\overline{W}$ would have a factorization into two relatively prime and nonlinear factors, and Theorem 5.6 would imply the existence of a similar factorization of W. □

3. The aim of this subsection is to show that every finite extension of a $\mathfrak{p}$-adic field is also a $\mathfrak{p}$-adic field, and, moreover, that $\mathfrak{p}$-adic fields can be characterized as those fields of zero characteristic which are complete with respect to a discrete valuation, and have a finite residue class field R/P, where R is the valuation ring and P the valuation ideal. Proposition 5.1 (i) shows that $\mathfrak{p}$-adic fields have those properties, and so we assume in this subsection that K is a field, satisfying the following three conditions:

(i) char $K = 0$,

(ii) *K is complete with respect to a discrete valuation v,*

(iii) *The field R/P, where R and P are the valuation ring and the valuation ideal, respectively, is finite.*

We start with a proposition which describes the prolongation of a discrete valuation to a finite extension.

Proposition 5.7. *If K satisfies (i) - (iii) and L/K is a finite extension, then there exists exactly one valuation w of L, which coincides with v on K. If $n = [L : K]$, then for $x \in L$ one has*

$$w(x) = v(N_{L/K}(x))^{1/n}.$$

Moreover L satisfies the conditions (i) - (iii).

Proof : Denote by S the integral closure of R in L. By Theorems 1.20 and 1.26 S is a Dedekind domain, whence if P_1 is a prime ideal of S lying above P, then the valuation w associated with it extends v after a suitable normalization. If w' is another extension of v to L, then by Proposition 3.2 they both induce the product topology in L, and so Proposition 1.23 implies $w = w'$. This gives us both existence and uniqueness of the extension. By Theorem 1.20 the ring S has the finite norm property, and Proposition 1.27 (iv) shows that the same holds for the valuation ring of w, giving (iii). Since (i) and (ii) are satisfied, because L is complete in the product topology, it remains to show that w has the asserted form. To do this let M/K be the minimal normal extension containing L in a fixed algebraic closure of L, and denote by u the unique extension of v to M. If $\sigma \in Gal(M/K)$, then putting $f(x) = u(\sigma(x))$ for $x \in M$, we obtain again an extension of v to M, and thus $f = u$. Since with suitable $\sigma_1, \ldots, \sigma_n \in Gal(M/K)$ we have

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x),$$

one gets for every $x \in L$ the equality

$$v(N_{L/K}(x)) = u(N_{L/K}(x)) = \prod_{i=1}^{n} u(\sigma_i(x)) = u(x)^n = w(x)^n. \quad \square$$

Corollary 1. *If K satisfies (i) - (iii) and L/K is finite, S denotes the valuation ring of the extension of v to L and $x \in L$, then the conditions $x \in S$ and $N_{L/K}(x) \in R$ are equivalent.* $\square$

Corollary 2. *If K satisfies (i) - (iii) and L/K is finite and normal, then every automorphism $\sigma \in Gal(L/K)$ is continuous in the topology induced by the extensions w of v to L.*

Proof : If for $x \in L$ we put $w'(x) = w(\sigma(x))$, then by the proposition we get $w' = w$, i.e., σ is an isometry. $\square$

Corollary 3. *If K is a field satisfying (i) - (iii), then the valuation v has a unique extension to the algebraic closure $\hat{K}$ of K.*

Proof : If $a \in \hat{K}$, then the field $L = K(a)$ is a finite extension of K, hence by the proposition there exists a unique extension w of v to L. Observe now that if M/K is a finite extension containing a and contained in $\hat{K}$, and w' is the unique extension of v to M, then w' is also an extension of w, and we get $w'(a) = w(a)$. This shows that by putting $V(a) = w(a)$ we define a valuation on $\hat{K}$, extending v, and it is obvious that V is the only extension of v to $\hat{K}$. $\square$

The valuation defined in Corollary 3 will be not discrete, and the field $\hat{K}$ will be not complete with respect to it, but since this will not be used in the sequel, we omit the proof. The interested reader is referred to Ostrowski [17].

Our next result, known as *Krasner's lemma*, is simple, but very useful.

Proposition 5.8. *Let K be a field satisfying (i) - (iii), and let the extension L/K be finite and normal. Denote by w the extension of v to L, and let $a \in L$ and $M = K(a)$. If $b \in L$ satisfies $w(a-b) < w(\sigma(b)-b)$ for every $\sigma \in Gal(L/K)$ with $\sigma(b) \neq b$, then $b \in M$.*

Proof : If the assertion fails, then there exists $\sigma \in Gal(L/K)$ with $\sigma(b) \neq b$ and $\sigma(a) = a$. But then

$$\begin{aligned} w(b-\sigma(b)) &= w(b-a+a-\sigma(b)) \leq \max\{w(b-a), w(a-\sigma(b))\} \\ &= \max\{w(b-a), w(\sigma(a)-\sigma(b))\} = w(b-a) < w(\sigma(b)-b), \end{aligned}$$

giving a contradiction. □

With the aid of Krasner's lemma we shall now show that two monic irreducible polynomials of the same degree, whose corresponding coefficients are sufficiently close to each other, define the same extension.

Proposition 5.9. *Let K be a field satisfying (i) - (iii), and let $F \in R[X]$ be a monic polynomial of degree n, irreducible over K. If $G \in R[X]$ is another monic polynomial of the same degree, whose coefficients are sufficiently close to the corresponding coefficients of F, then G is irreducible over K, and to every root α of F in a fixed algebraic closure $\hat{K}$ of K there corresponds a root $\beta \in \hat{K}$ of G such that the fields $K(\alpha)$ and $K(\beta)$ coincide.*

Proof : We shall denote the extension of v to $\hat{K}$ by the same letter v. Let $F(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ and $G(X) = X^n + \sum_{i=0}^{n-1} b_i X^i$. We prove first that if $\delta > 0$ is given and $\max_i v(a_i - b_i)$ is sufficiently small, then to every root α of F there exists a root β of G such that $v(\alpha - \beta) < \delta$. Let $\alpha \in \hat{K}$ be a given root of F, and let $\beta_1, \ldots, \beta_n$ be the roots of G in $\hat{K}$, each of them occurring in this sequence according to its multiplicity. Assume, to the contrary, that for $i = 1, 2, \ldots, n$ we have $v(\alpha - \beta_i) \geq \delta$. In view of $G(X) = (X - \beta_1) \cdots (X - \beta_n)$ we get

$$v(G(\alpha)) = \prod_{i=1}^{n} v(\alpha - \beta_i) \geq \delta^n,$$

hence

$$v(F(\alpha) - G(\alpha)) = v(G(\alpha)) \geq \delta^n.$$

On the other hand, we have

$$F(\alpha) - G(\alpha) = \sum_{j=0}^{n-1} (a_j - b_j)\alpha^j,$$

thus

$$v(F(\alpha) - G(\alpha)) \leq \max_j v(a_j - b_j) v(\alpha^j),$$

and finally

$$\delta^n \leq B \max_j v(a_j - b_j),$$

with $B = \max_j v(\alpha)^j$. However the last inequality is impossible if $v(a_j - b_j)$ is sufficiently small for $j = 0, 1, \ldots, n-1$.

Now let $\alpha_1, \ldots, \alpha_n$ be all the roots of F in $\hat{K}$, and put

$$\delta = \min_{i \neq j} v(\alpha_i - \alpha_j).$$

If the coefficients of G are sufficiently close to the corresponding coefficients of F, then to every α_i there corresponds a root β_i of G with $v(\alpha_i - \beta_i) < \delta$.

Applying Proposition 5.8 to the smallest normal extension of K, containing the splitting field of F and all the β_i's, we get $\alpha_i \in K(\beta_i)$, thus $K(\alpha_i) \subset K(\beta_i)$. Since $[K(\alpha_i) : K] = n$ and $[K(\beta_i) : K] \leq n$, we get $K(\alpha_i) = K(\beta_i)$, and the irreducibility of G follows immediately. □

Now we prove a characterization of $\mathfrak{p}$-adic fields:

Theorem 5.10. *Let K be a field with a valuation v. The following properties are equivalent:*

(a) K is a $\mathfrak{p}$-adic field with the $\mathfrak{p}$-adic valuation,

(b) K satisfies the conditions (i) - (iii),

(c) K is a finite extension of $\mathbb{Q}_p$ for a suitable prime p.

Proof : We know already that the implication (a)⇒ (*b*) is true. Assume now (b), hence K satisfies (i) - (iii). The restriction of v to the field of rational numbers is discrete, thus Theorem 1.31 shows that it is equivalent to a certain p-adic valuation. Since K is complete, Theorem 3.1 implies that K contains an isomorphic copy of some field $\mathbb{Q}_p$, and v restricted to $\mathbb{Q}_p$ coincides with its usual valuation (after a suitable renormalization, if required). We may simply assume that $\mathbb{Q}_p \subset K$. Let ν be the exponent of K, induced by v, and put $e = \nu(p)$. Then e is a non-zero rational integer and we have $pR = P^e$. Now choose $\pi \in P \setminus P^2$, and put $t_{je+r} = p^j \pi^r$ for $j = 0, 1, \ldots$, $r = 0, 1, \ldots, e-1$. Moreover let the set $\Omega = \{\omega_1, \ldots, \omega_f\} \subset R$ (with $p^f = \#R/P$) have the property that the elements $\omega_i \bmod P$ form a basis of the field R/P, treated as a linear $\mathbb{F}_p$-space. A simple argument, utilizing Theorem 5.2, shows now that R is freely generated, as an $\mathbb{Z}_p$-module, by the elements $\omega_i \pi^r$ $(i = 1, 2, \ldots, f; r = 0, 1, \ldots, e-1)$. In particular R is a finitely generated free $\mathbb{Z}_p$-module, hence K has a finite dimension as a linear $\mathbb{Q}_p$-space. This establishes (c).

Finally assume (c) and let $K = \mathbb{Q}_p(a)$ with $a \in R$. The coefficients of the minimal polynomial of a over $\mathbb{Z}_p$ may be approximated arbitrarily close by rational integers. If we replace these coefficients (except the leading term, which should be 1) by those approximants, we obtain a polynomial over $\mathbb{Z}$ which, by Proposition 5.9, will be irreducible over $\mathbb{Q}_p$, and one of its roots, say b, will generate K over $\mathbb{Q}_p$. The field $L = \mathbb{Q}(b)$ is a finite extension of $\mathbb{Q}$ contained in K. Observe now that the valuation v of K induces in L a discrete valuation which, by Theorem 3.3, is induced by a prime ideal $\mathfrak{p}$ of R_L, and we obtain $K = L_{\mathfrak{p}}$. □

4. The next theorem enables us to translate several problems concerning finite extensions of algebraic number fields into the language of $\mathfrak{p}$-adic fields. Its applications will be discussed in the next chapter.

Theorem 5.11. *Let K be an algebraic number field, $\mathfrak{p}$ a non-zero prime ideal of R_K, and $K_{\mathfrak{p}}$ the completion of K, corresponding to $\mathfrak{p}$. Moreover, let L/K*

be an extension of degree n, $\mathfrak{P}$ a prime ideal of R_L lying above $\mathfrak{p}$, and $L_{\mathfrak{P}}$ the corresponding completion. Finally, let R and S be the rings of integers in $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$, respectively. Then we have:

(i) $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = e_{L/K}(\mathfrak{P}) f_{L/K}(\mathfrak{P})$,

(ii) The field $L_{\mathfrak{P}}$ is the composite of L and $K_{\mathfrak{p}}$,

(iii) The ring S is the integral closure of R in $L_{\mathfrak{P}}$,

(iv) If $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{P}}$ are the prime ideals of R and S, respectively, then $\overline{\mathfrak{P}}$ lies over $\overline{\mathfrak{p}}$ and $e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\overline{\mathfrak{P}}) = e_{L/K}(\mathfrak{P})$, $f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\overline{\mathfrak{P}}) = f_{L/K}(\mathfrak{P})$,

Proof : We need a lemma:

Lemma 5.12. *Under the assumptions of Theorem 5.11 we have:*

(i) The extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is finite.

(ii) The ring S is the integral closure of R in $L_{\mathfrak{P}}$.

(iii) For every ideal I of R one has

$$N(IS) = N(I)^M,$$

where $M = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$.

Proof : (i) The closure of K in $L_{\mathfrak{P}}$ is complete, and so, in view of Theorem 3.1, we may identify it with $K_{\mathfrak{p}}$. Let $a_1, \ldots, a_n$ be a basis of the K-space L, and observe that

$$L_1 = a_1 K_{\mathfrak{p}} + a_2 K_{\mathfrak{p}} + \cdots + a_n K_{\mathfrak{p}}$$

is a $K_{\mathfrak{p}}$-space, contained in $L_{\mathfrak{P}}$ and containing L. Moreover we have

$$\dim_{K_{\mathfrak{p}}} L_1 \leq n = \dim_K L.$$

By Proposition 3.2 L_1 has the product topology, hence it is closed, and this implies $L_1 = L_{\mathfrak{P}}$. This shows $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] \leq n < \infty$.

(ii) Let $a \in S$. By Proposition 5.1 (ii) there is a sequence $x_1, x_2 \ldots$ of elements of R_L converging to a. Let

$$F_m(X) = X^n + \sum_{j=0}^{n-1} c_j^{(m)} X^j$$

be a polynomial over R_K, having x_m for one of its roots. (If x_m generates L over K, then F_m is the minimal polynomial of x_m, otherwise F_m is the product of the minimal polynomial and a suitable power of X). From every sequence $\{c_j^{(m)}\}$ we can extract a subsequence, converging in R to c_j, say. If now $F(X) = X^n + \sum_{j=0}^{n-1} c_j X^j$, then obviously $F(a) = 0$, showing that a is integral over R. Thus S is contained in the integral closure of R in $L_{\mathfrak{P}}$, but S is integrally closed, and (ii) follows.

(iii) Let $\overline{\mathfrak{P}}$, $\overline{\mathfrak{p}}$ be the prime ideals of S and R, respectively. Proposition 5.1 (i) shows that R is a principal ideal domain, and since S is a torsion-free, finitely generated R-module there exist elements $\omega_1, \ldots, \omega_M \in S$ such that every $x \in S$ can be uniquely written in the form $x = \sum_{i=1}^{M} x_i \omega_i$ with $x_i \in R$.

If now $m = N(\overline{\mathfrak{p}})$, and $A = \{a_1, \ldots, a_m\}$ is a set of representatives of R mod $\mathfrak{p}$, then the set $\{\sum_{j=1}^{M} \alpha_j \omega_j : \alpha_j \in A\}$ is a set of representatives of S mod $\overline{\mathfrak{p}}S$. Indeed, if $\xi = \sum_{j=1}^{M} \xi_j \omega_j \in S$ ($\xi_j \in R$), then we may write $\xi_j = \alpha_j + \beta_j$ with $\alpha_j \in A$ and $\beta_j \in \overline{\mathfrak{p}}$ to get

$$\xi - \sum_{j=1}^{M} \alpha_j \omega_j \in \overline{\mathfrak{p}}S.$$

On the other hand, if

$$\sum_{j=1}^{M} \alpha_j \omega_j \equiv \sum_{j=1}^{M} \beta_j \omega_j \pmod{\overline{\mathfrak{p}}S}$$

where $\alpha_j, \beta_j \in A$, and π is the generator of $\overline{\mathfrak{p}}$, then

$$\sum_{j=1}^{M} \frac{\alpha_j - \beta_j}{\pi} \omega_j \in S,$$

implying $\alpha_j \equiv \beta_j \pmod{\overline{\mathfrak{p}}}$ and $\alpha_j = \beta_j$ for $j = 1, \ldots, M$. This implies $N(\overline{\mathfrak{p}}S) = N(\overline{\mathfrak{p}})^M$. The assertion (iii) follows now from Theorem 1.16 (i), and the observation that every non-zero ideal in R is a power of the unique prime ideal. □

We return to the proof of the theorem. The assertion (ii) follows from the observation that the fields $K_{\mathfrak{p}}$ and L generate the linear space L_1, occurring in part (i) of the preceding lemma. Part (iii) of the theorem is contained in Lemma 5.12 (ii), and to obtain the remaining parts observe that Proposition 5.1 shows that $\overline{\mathfrak{P}}$ is the only non-zero prime ideal of S, and so it must lie above $\overline{\mathfrak{p}}$. Lemma 5.12 (iii) shows that Theorem 4.5 is applicable, and therefore we get $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$, where $e = e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\overline{\mathfrak{P}})$, $f = f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\overline{\mathfrak{P}})$. The equality $f = f_{L/K}(\mathfrak{P})$ follows from Proposition 5.1 (i). Since $\mathfrak{p}R_L = \mathfrak{P}^{e_1}\mathfrak{Q}$ holds with $e_1 = e_{L/K}(\mathfrak{P})$, and $\mathfrak{P} \nmid \mathfrak{Q}$, hence taking closures we get $\overline{\mathfrak{p}}S = \overline{\mathfrak{P}}^{e_1}\mathfrak{Q}_1$, $\mathfrak{Q}_1$ being the closure of $\mathfrak{Q}$. Since $\mathfrak{Q}_1$ is not divisible by $\overline{\mathfrak{P}}$, it contains an element which does not lie in $\overline{\mathfrak{P}}$, and is a unit in S, whence $\mathfrak{Q}_1 = S$, and we get $\overline{\mathfrak{P}}^{e} = \overline{\mathfrak{p}}S = \overline{\mathfrak{P}}^{e_1}$, thus $e = e_1$. This proves (iv), and (i) follows immediately. □

We point out a useful corollary:

Corollary. *If L_1, L_2 are finite extensions of an algebraic number field K, and $\mathfrak{p}$ is a prime ideal of R_K, splitting in L_1 and L_2, then it splits also in their composite L_1L_2.*

Proof: Let $\mathfrak{P}$ be a prime ideal lying over $\mathfrak{p}$ in $L = L_1L_2$, and put $\mathfrak{P}_i = \mathfrak{P} \cap R_{L_i}$ $(i = 1, 2)$. By (i) we have the equality $[(L_i)_{\mathfrak{P}_i} : K_{\mathfrak{p}}] = 1$ for $i = 1, 2$, whence both fields L_i are contained in $K_{\mathfrak{p}}$. Thus $L = L_1L_2 \subset K_{\mathfrak{p}}$, and we obtain that $L_{\mathfrak{P}}$, being the closure of L, is a subset of $K_{\mathfrak{p}}$. Therefore $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 1$, and we get from (i) the equalities

$$e_{L/K}(\mathfrak{P}) = f_{L/K}(\mathfrak{P}) = 1,$$

as asserted. □

We see that the behaviour of the prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ is the same as that of $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{P}}$. Moreover, one sees easily that $\overline{\mathfrak{P}} = \mathfrak{P}S$ and $\overline{\mathfrak{p}} = \mathfrak{p}R$, and so we can dispense with the pedantic distinguishing between $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, $\mathfrak{P}$ and $\overline{\mathfrak{P}}$. In the sequel we shall thus use the same letter for a prime ideal in an algebraic number field and its closure in the corresponding completion.

Note, moreover, that as there is only one prime ideal in the ring of integers of a $\mathfrak{p}$-adic field, we can freely write $e(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ for $e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\mathfrak{P})$ and $f(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ for $f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\mathfrak{P})$, and speak about the ramification index or the residue class field degree of the extension rather than that of a prime ideal.

5. Lemma 5.12 (ii) implies that we can apply the theory developed in Chap. 4 to finite extensions of $\mathfrak{p}$-adic fields, and since the class-group of the ring of integers of a $\mathfrak{p}$-adic field is trivial, we can obtain more. In particular the following result shows that in the $\mathfrak{p}$-adic case every finite extension possesses a power integral basis:

Proposition 5.13. *If L/K is an extension of degree n of $\mathfrak{p}$-adic fields, and R, S are the corresponding rings of integers, then there exists $a \in S$ such that the R-module generated freely by $1, a, \ldots, a^{n-1}$ coincides with S, i.e., $S = R[a]$.*

Proof: It follows from Corollary to Lemma 4.20 that there exists $a \in S$ such that the conductor of the ring $R[a]$ is not divisible by $\mathfrak{P}$, hence this conductor equals S, and now Corollary to Proposition 4.18 shows that the R-modules $R[a]$ and S coincide. □

Now we shall define, following Fröhlich [60b], the numerical discriminant $\partial(L/K)$ for finite extensions L/K of $\mathfrak{p}$-adic fields. This discriminant will be very useful for the intended applications to algebraic number fields.

Let thus L/K be such an extension, and let R, S be the rings of integers in K and L, respectively. According to the preceding proposition S is a free

R-module, and for every set $\omega_1, \ldots, \omega_n$ of its free generators we define its discriminant $d_{L/K}(\omega_1, \ldots, \omega_n)$ by

$$d_{L/K}(\omega_1, \ldots, \omega_n) = \det \left[T_{L/K}(\omega_i \omega_j)\right],$$

or, equivalently, by

$$d_{L/K}(\omega_1, \ldots, \omega_n) = \left(\det \left[\omega_i^{(j)}\right]\right)^2,$$

where $\omega_i^{(j)}$ are the conjugates of ω_i in an algebraic closure of L. In the same way as was done in Chap. 2 in the case of algebraic number fields, we see that this discriminant is non-zero, and the discriminants of different sets of free generators of S differ by the square of a unit of R. Since in $\mathbb{Q}$ the only square of a unit was the unit element, we could then define the field discriminant as the common value of discriminants of sets of free generators. Now it is no longer possible to proceed in the same manner, and we define instead the discriminant $\partial(L/K)$ as the class in the factor group $K^*/U(K)^2$, which contains the discriminants of every system of free generators of S.

The next proposition lists the principal properties of the discriminant so defined:

Proposition 5.14. *Let L/K be an extension of degree n of the $\mathfrak{p}$-adic field K, and let R, S be the rings of integers of K and L, respectively.*

(i) The ideal in R, generated by any representative of $\partial(L/K)$ equals the discriminant $d(L/K)$, defined in Chap. 4,

(ii) The extension L/K is unramified if and only if $\partial(L/K)$ lies in $U(K)/U(K)^2$,

(iii) If M/L is an extension of degree m, then

$$\partial(M/K) = \partial(L/K)^m N_{L/K}(\partial(M/L)),$$

where the norm mapping is to be understood as acting from $L^*/U(L)^2$ to $K^*/U(K)^2$, which is allowed since the norm of a square of a unit is also a square of a unit.

Proof: Since every representative of $\partial(L/K)$ generates the same ideal, we can consider a set of generators of the form $1, a, \ldots, a^{n-1}$, which exists according to Proposition 5.13. In the same way as in the proof of Proposition 2.9 (iv) we find that the discriminant of this set generates the same ideal as the element $N_{L/K}(f'(a))$, where f is the minimal polynomial of a over R. By Corollary 1 to Proposition 4.8 and the observation that the different $D_{L/K}$ equals $f'(a)S$, we obtain (i).

Assertion (ii) follows from (i) and the discriminant theorem, so it remains to establish (iii). To do this let $a_1, \ldots, a_n$ be a set of free generators of S as an R-module, and let $b_1, \ldots, b_m$ be a set of free generators of the ring T of integers of M as a S-module. One sees easily that the set of all products

$a_i b_j$ form a set of free generators of T as an R-module, and we shall use it to compute the discriminant $\partial(M/K)$. Let N be a normal extension of K containing M, let $T_1 = \{t_1, \ldots, t_n\}$ be the set of all embeddings of L in N, fixing K, and extended to automorphisms of N, and, similarly, let $T_2 = \{s_1, \ldots, s_m\}$ be the set of all automorphisms of N, fixing L. Consider the matrices $A = [t(a_i)]$ $(t \in T_1, i = 1, 2, \ldots, n)$ and $B = [s(b_j)]$ $(s \in T_2$, $i = 1, 2, \ldots, m)$. We have obviously

$$\partial(L/K) = (\det A)^2 \bmod U(K)^2$$

and

$$\partial(M/L) = (\det B)^2 \bmod U(L)^2.$$

Moreover, if C denotes the $mn \times mn$ matrix $[t_k(a_i)t_k(s_l(b_j))]_{(k,l),(i,j)}$, then

$$\partial(M/K) = (\det C)^2 \bmod U(K)^2.$$

To find the relations between the determinants of the matrices A, B and C write

$$A_1 = \left[t_k(a_i)\delta_i^j\right]_{(k,l),(i,j)},$$

and

$$B_1 = \left[t_k(s_l(b_j))\delta_i^k\right]_{(k,l),(i,j},$$

and observe that $B_1 A_1 = C$. In view of

$$\det A_1 = \pm(\det A)^m, \quad \det B_1 = \pm N_{L/K}(\det B),$$

we obtain the following chain of equalities mod $U(K)^2$:

$$\begin{aligned}\partial(M/K) = (\det C)^2 &= (\det A_1)^2(\det B_1)^2 = (\det A)^{2m} N_{L/K}^2(\det B) \\ &= \partial(L/K)^m N_{L/K}(\partial(M/L)),\end{aligned}$$

as asserted. □

To give an example let us compute the discriminants of quadratic extensions:

Theorem 5.15. *Let K be a $\mathfrak{p}$-adic field, R its ring of integers, $\mathfrak{p}$ its prime ideal, and a an element of R which is not a square in K, and which does not lie in $\mathfrak{p}^2$. Moreover choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. If $L = K(\sqrt{a})$ and S is the ring of integers of L, then the following possibilities arise:*

(i) If $\pi \nmid 2a$, then

$$S = R[\sqrt{a}], \qquad \partial(L/K) = a \bmod U(K)^2,$$

(ii) If $\pi | a$, then

$$S = R[\sqrt{a}], \qquad \partial(L/K) = 4a \bmod U(K)^2,$$

(iii) If $\pi|2$, $\pi \nmid a$, and the congruence

$$X^2 \equiv a \pmod{\mathfrak{p}^2}$$

has no solutions in R, then

$$S = R[\sqrt{a}], \qquad \partial(L/K) = 4a \bmod U(K)^2,$$

(iv) If $\pi|2$, $\pi \nmid a$, and l is the largest positive integer such that $\pi^l|2$ and the congruence

$$X^2 \equiv a \pmod{\mathfrak{p}^{2l}} \tag{5.4}$$

has a solution in R, then

$$S = R[(b + \sqrt{a})\pi^{-l}] \qquad \partial(L/K) = 4a\pi^{-2l} \bmod U(K)^2,$$

where b is a solution of (5.4).

Proof : By Proposition 5.13 we have $S = R[c]$ with a certain $c \in S$, which in any case can be written in the form

$$c = \frac{x + y\sqrt{a}}{\pi^k} \quad (x, y \in R, k \geq 0), \tag{5.5}$$

and without restricting the generality we may assume that $(x, y, \pi) = 1$.

We start with the case (i). Note that the norm $N_{L/K}(c) = (x^2 - ay^2)\pi^{-2k}$ lies in R, and thus if k is positive, then the congruence

$$X^2 \equiv aY^2 \pmod{\mathfrak{p}}$$

is solvable in R with $X, Y \notin \mathfrak{p}$, and this shows that the congruence $X^2 \equiv a \pmod{\mathfrak{p}}$ has a solution in R. By Corollary 1 to Theorem 5.6 this implies (in view of $2a \notin \mathfrak{p}$) that a is a square in K, contrary to our assumption. Thus $k = 0$ and $c = x + y\sqrt{a}$ with $x, y \in R$. This gives

$$S = R \oplus (x + y\sqrt{a}) \subset R[\sqrt{a}] \subset S,$$

thus $S = R[\sqrt{a}]$. Moreover, we have $\partial(L/K) = 4a \bmod U(K)^2$, and in view of $2 \in U(K)$ we arrive at $\partial(L/K) = a \bmod U(K)^2$.

Now consider the case (ii), and let ν be the exponent associated with the prime ideal $\mathfrak{p}$. Since $\nu(a) \geq 1$ and $\pi^2 \nmid a$, we must have $\nu(a) = 1$, thus Proposition 1.24 implies $\nu(x^2 - ay^2) = r = \min\{2\nu(x), 1 + 2\nu(y)\}$, and in view of $N_{L/K}(c) \in R$ we obtain $2k \leq r$. Since one of the numbers $\nu(x)$, $\nu(y)$ is zero, we get $k = 0$, and proceeding in the same way as in the case (i) we obtain $S = R[\sqrt{a}]$ and $\partial(L/K) = 4a \bmod U(K)^2$.

In the case (iii) observe that if $k \geq 1$, then $N(c) = (x^2 - y^2a)/\pi^2 \in R$, so $x^2 \equiv y^2a \,(\mathrm{mod}\, \pi^2)$, and in view of $\pi \nmid xy$ the congruence $X^2 \equiv a \pmod{\pi^2}$ has a solution in R, contrary to our assumption. Therefore $k = 0$, hence $c = x + y\sqrt{a}$, and the assertion follows an in case (i).

We are left with the case (iv). In this case our assumption implies $k \geq 1$, and since $N(c) = (x^2 - y^2 a)/\pi^{2k} \in R$ and $\pi \mid (x, y)$ we get $\pi \nmid xy$. As

$$\partial(L/K) = 4y^2 a\pi^{-2k} = 4a\pi^{-2k} \bmod U(K)^2,$$

it remains to show that $k = l$. Since $\pi^{2k} | 4ay^2$ and $\pi \nmid ay$, we obtain $\pi^{2k} | 4$, thus $\nu(2) \geq k$. Moreover, (5.4) is satisfied with $l = k$ by $X = xy'$, where $yy' \equiv 1 \,(\mathrm{mod}\ \mathfrak{p}^{2k})$. Finally we prove that no number $m > k$ has the required properties. In fact, if for a certain $t \in R$ we have $t^2 \equiv a \,(\mathrm{mod}\ \mathfrak{p}^{2m})$, then $(t + \sqrt{a})\pi^{-m}$ lies in S, and it follows that for suitable $A, B \in R$ we have

$$(t + \sqrt{a})\pi^{-m} = A + B(x + y\sqrt{a})\pi^{-k},$$

hence $\pi^{k-m} = By \in R$ and $k \geq m$. □

Note that this theorem actually covers all quadratic extensions of a $\mathfrak{p}$-adic field, since every such extension has a generator $\sqrt{a}$ with $a \in R$ and $0 \leq \nu(a) \leq 1$, because if $a = \epsilon\pi^m$ with $\epsilon \in U(K)$ and $m \geq 2$, then $\sqrt{a}$ defines the same extension as $\sqrt{\epsilon}$ or $\sqrt{\epsilon\pi}$, depending on the parity of m.

Corollary. *Let K be a $\mathfrak{p}$-adic field, and let $L = K(\sqrt{a})$ with $0 \leq \nu(a) \leq 1$. Then the extension L/K is unramified if and only if either K is not an extension of $\mathbb{Q}_2$ and a is a unit, or K is an extension of $\mathbb{Q}_2$, a is a unit, and the congruence $X^2 \equiv a \,(\mathrm{mod}\ 4)$ has a solution in R, the ring of integers of K.*

Proof : Apply Proposition 5.14 (ii) and the theorem just proved. □

6. Now let us have a closer look at the group of units. Let K be a $\mathfrak{p}$-adic field, R its ring of integers with the prime ideal $\mathfrak{p}$, v the valuation of K, ν the associated exponent, π a fixed element of $\mathfrak{p} \setminus \mathfrak{p}^2$, p the characteristic of the residue class field $k = R/\mathfrak{p}$ (thus $\mathbb{Q}_p \subset K$), e the ramification index of $K/\mathbb{Q}_p$, f the degree of $\mathfrak{p}$ over $\mathbb{Q}_p$, i.e., $f = [k : \mathbb{F}_p]$, and finally let $U = U(K)$ be the group of units of K. We shall consider also certain subgroups of U: the group $E(K)$ of all roots of unity, contained in K, its subgroup $E_1(K)$, whose elements are roots of unity of order $p^f - 1$, and the groups $U_m = U_m(K)$ $(m \geq 1)$ consisting of all units u, congruent to unity mod $\mathfrak{p}^m$. The group U_1 is called the *group of principal units of K*. Note that the intersection $U_1(K) \cap E(K)$ may be non-trivial, as the example $K = \mathbb{Q}_2(\sqrt{-1})$ shows, in which case $\sqrt{-1} \in E(K) \cap U_1(K)$. On the other hand, one has $E_1(K) \cap U_1(K) = \{1\}$. The group $E_1(K)$ forms the uninteresting factor in the decomposition given in the next result:

Proposition 5.16. *For every $\mathfrak{p}$-adic field K we have*

$$U(K) = E_1(K) \times U_1(K).$$

Proof : Apply Corollary 2 to Theorem 5.6 and the preceding remark. □

Corollary 1. *The multiplicative group of a $\mathfrak{p}$-adic field K is the product of $E_1(K)$, $U_1(K)$ and the infinite cyclic group.*

Proof : Apply Proposition 5.1 (ii) and 5.16. □

Corollary 2. *One has $U(K)/U_1(K) \sim k^*$.*

Proof : Both groups are cyclic and have $p^f - 1$ elements. □

Now let us consider the groups U_m,

Proposition 5.17. *(i) The groups U_m form a basis of open neighbourhoods of the unit element in the group K^* and are compact.*

(ii) For $m = 1, 2, \ldots$ the factor group U_m/U_{m+1} is isomorphic to the additive group of $\mathbb{F}_{p^f}$.

(iii) For $m = 1, 2, \ldots$ the factor group $U(K)/U_m(K)$ is isomorphic to the group of invertible elements of the factor ring $R/\mathfrak{p}^m$.

Proof : The assertion (i) is immediate, and to show (ii) define a mapping ψ of the additive group of $\mathfrak{p}^m$ into U_m/U_{m+1} by putting

$$\psi(x) = 1 + x \bmod U_{m+1}.$$

Since

$$\psi(x+y) = 1 + x + y \bmod U_{m+1} = (1+x)(1+y) \bmod U_{m+1} = \psi(x)\psi(y),$$

ψ is a group homomorphism, which is clearly surjective, and has $\mathfrak{p}^{m+1}$ for its kernel. Thus U_m/U_{m+1} and $(\mathfrak{p}^m)^+/(\mathfrak{p}^{m+1})^+$ are isomorphic, and it remains to apply Lemma 1.17.

To prove (iii) put for $u \in U(K)$ $\phi(u) = u \bmod \pi^m$. Clearly ϕ is a surjective homomorphism of $U(K)$ onto $(R/\mathfrak{p}^m)^*$, and $\ker \phi = U_m$. □

Corollary. *The quotient U_m/U_{m+1} is the f-th power of C_p, the cyclic group of p elements.*

Proof : Observe that k is an f-dimensional linear space over $\mathbb{F}_p$. □

The group U_1 can be considered as a $\mathbb{Z}_p$-module. To establish this let ϵ be a principal unit, and let $a = a_0 + a_1 p + \cdots$ $(0 \leq a_i \leq p-1)$ be an element of $\mathbb{Z}_p$. Consider the sequence

$$\epsilon_n = \epsilon^{a_0 + a_1 + \cdots + a_n p^n},$$

and observe that for $n > m$ we have

$$v(\epsilon_n - \epsilon_m) = v\left(\epsilon^{a_{m+1}p^{m+1}+\cdots+a_np^n} - 1\right).$$

A short calculation shows that the last expression converges to zero when m tends to infinity, and thus by completeness the sequence $\{\epsilon_n\}$ has a limit, say η. Since U_1 is closed, we have $\eta \in U_1$. This shows that by putting $\epsilon^a = \eta$ one defines an action of $\mathbb{Z}_p$ on U_1, and now it is easy to check that in this way U_1 becomes a $\mathbb{Z}_p$-module.

To obtain a description of the $\mathbb{Z}_p$-module U_1 we need some auxiliary results.

Lemma 5.18. *If k is a rational integer not divisible by p, then every element $\epsilon \in U_1$ has a k-th root lying in U_1.*

Proof : It suffices to observe that $1/k \in \mathbb{Z}_p$. □

Lemma 5.19. *If $m > e/(p-1)$ and $u \in U_{m+e}$, then the polynomial $X^p - u$ has a root in U_m.*

Proof : Write $u = 1 + a\pi^{m+e}$ with $a \in R$, and let $b = 1 + c\pi^m$ (with $c \in R$) be an arbitrary element of U_m. Then

$$b^p - u = (1 + c\pi^m)^p - (1 + a\pi^{m+e}) = \sum_{j=1}^{p} \binom{p}{j} c^j \pi^{mj} - a\pi^{m+e}.$$

Since $\nu(p) = e$, we have

$$\nu\left(\binom{p}{j} c^j \pi^{mj}\right) \geq \left\{ \begin{array}{ll} e + mj & \text{if } 1 \leq j \leq p-1, \\ mp & \text{if } j = p \end{array} \right\} \geq m + e,$$

hence writing $p = \epsilon\pi^e$ with a certain unit ϵ we obtain finally

$$(b^p - u)\pi^{-m-e} = V(c) + \epsilon c - a,$$

where $V \in \mathfrak{p}[X]$. It follows that to solve the equation $X^p - u = 0$ in U_m it suffices to find a root of the polynomial $W(X) = V(X) + \epsilon X - a$ in R. But after reducing W mod $\mathfrak{p}$ we get a non-constant linear polynomial over k, and the application of Corollary 1 to Theorem 5.6 gives what is needed. □

Corollary. *If $m > e/(p-1)$ then the groups U_m and U_{m+e} are isomorphic. This isomorphism is given by the map $g : U_m \longrightarrow U_{m+e}$ defined by $g(u) = u^p$.*

Proof : If $u = 1 + a\pi^m \in U_m$ with a non-zero $a \in R$, then

$$u^p = 1 + \sum_{j=1}^{p} \binom{p}{j} a^j \pi^{jm},$$

and since the minimal value of $\nu\left(\binom{p}{j}a^j\pi^{jm}\right)$ for $j = 1, 2, \ldots, p$ is attained only at $j = 1$, and is $\geq e + m$, we get $g(U_m) \subset U_{m+e}$, and $\nu(u^p - 1) = m + \nu(\binom{p}{j}a^j)$. This shows that $u^p \neq 1$, thus g is injective, and its surjectivity follows from the lemma. □

The next lemma is of a general nature.

Lemma 5.20. *Let $A = A_0 \supset A_1 \supset A_2 \supset \ldots$ and $B = B_0 \supset B_1 \supset B_2 \supset \ldots$ be two descending sequences of Abelian groups, such that the quotient groups A/A_n and B/B_n are all finite. Assume that $A \sim \liminv A/A_n$ and $B \sim \liminv B/B_n$, the isomorphism being given by the canonical maps*

$$a \mapsto [a \bmod A_1, a \bmod A_2, \ldots] \quad (a \in A),$$

$$b \mapsto [b \bmod B_1, b \bmod B_2, \ldots] \quad (b \in B).$$

Let $f : A \longrightarrow B$ be a homomorphism mapping each A_n into the corresponding B_n, and assume that all the induced homomorphisms

$$f_n : A_n/A_{n+1} \longrightarrow B_n/B_{n+1}$$

are injective, or surjective, or bijective. Then the same holds for f.

Proof : The groups A and B are inverse limits of finite groups, and therefore they acquire a topology in which they are both compact and complete.

Assume first that all homomorphisms f_n are injective, and let $x \in \operatorname{Ker} f$. Since $\bigcap_n A_n = \{0\}$ hence if $x \neq 0$, then for a suitable n we have $x \in A_n \setminus A_{n+1}$. Moreover from $f(x) = 0$ we infer that $f_n(x \bmod A_{n+1}) = 0$, and as f_n is injective we obtain $x \in A_{n+1}$, contradiction. Thus $\operatorname{Ker} f = 0$ and f is injective.

Now assume that each f_n is surjective. Our assumptions imply that A and B are complete topological groups with A_n and B_n forming bases of open neighbourhoods of the zero element in A and B, respectively. Therefore if $\{a_m\}$ is a sequence of elements of A such that for sufficiently large m and any $n > m$ the difference $a_n - a_m$ lies in a given set A_N, then that sequence is convergent, and the same applies to B. Now let $y_0 \in B$ be given. If $y_0 = 0$, then $f(0) = y_0$. Otherwise there exists an n with $y_0 \in B_n \setminus B_{n+1}$, because $\bigcap_n B_n = \{0\}$. By the surjectivity of f_n there exist $x_1 \in A_n$, $y_1 \in B_n$ with $y_0 = f(x_1) + y_1$. Similarly we obtain $x_2 \in A_{n+1}$ and $y_2 \in B_{n+1}$ such that $y_1 = f(x_2) + y_2$, and proceeding in this way we obtain a sequence $x_1, x_2, \ldots$ of elements of A, and a sequence $y_1, y_2, \ldots$ of elements of B which satisfy $x_k \in A_{n+k-1}$, $y_k \in B_{n+k-1}$, and are related by

$$y_k = f(x_{k+1}) + y_{k+1} \quad (k = 0, 1, \ldots).$$

Now put $z_k = \sum_{j=1}^{k} x_j$, and observe that the sequence $\{z_k\}$ is fundamental in A, thus convergent to a certain $x \in A$. Note also that f is continuous, since for every n the inclusion $f(x) \in B_n$ implies $f(x + A_n) \subset B_n$. Thus

$$y_0 = \lim_k (y_0 - y_k) = \lim_k \sum_{j=1}^{k} f(x_j) = \lim_k f(z_k) = f(x),$$

and so f is surjective. □

Now we can describe the structure of the $\mathbb{Z}_p$-module $U_1(K)$:

Theorem 5.21. *Let K be a $\mathfrak{p}$-adic field of degree n over $\mathbb{Q}_p$, and let $s \geq 0$ be the maximal exponent with the property that K contains a primitive p^s-th root of unity. Then $U_1(K)$ is a direct sum of a free $\mathbb{Z}_p$-module of rank $[K : \mathbb{Q}_p]$, and a cyclic group of order p^s, on which $\mathbb{Z}_p$ acts by $x^a = x^{a \bmod p^s}$.*

(The exponent s is called the *index of irregularity* of K. The field K is called *regular* if $s = 0$ and *irregular* otherwise).

Proof : Let $e = e(K/\mathbb{Q}_p)$. The Corollary to Lemma 5.19 implies that for $m > e/(p-1)$ we have $U_m^p \subset U_{m+e}$, therefore the factor group U_m/U_{m+e} can be regarded as a vector space over $\mathbb{F}_p$, an element $a \in \mathbb{F}_p$ acting on $x \in U_m/U_{m+e}$ by $a \cdot x = x^a$. In view of $\#U_m/U_{m+e} = p^{ef}$, this implies $U_m/U_{m+e} \sim C_p^n$. Applying Theorem V of Appendix I we see that U_m is the inverse limit of the family U_m/U_{m+ke} $(k = 1, 2, \ldots)$ of groups.

Let $x_1, \ldots, x_n$ be the generators of U_m mod U_{m+e}, and consider the map $f : \mathbb{Z}_p^m \longrightarrow U_m$, defined by

$$f([a_1, \ldots, a_n]) = x_1^{a_1} \cdots x_n^{a_n}.$$

If for a certain k we have $[a_1, \ldots, a_n] \in (p^k\mathbb{Z}_p)^n$, then

$$f([a_1, \ldots, a_n]) = x_1^{b_1 p^k} \cdots x_n^{b_n p^k}$$

with suitable $b_i \in \mathbb{Z}_p$. Thus f maps $(p^k\mathbb{Z}_p)^n$ in U_{m+ke}, and the Corollary to Lemma 5.19 shows that the homomorphisms

$$f_k : (p^k\mathbb{Z}_p)^n/(p^{k+1}\mathbb{Z}_p)^n \longrightarrow U_{m+ke}/U_{m+(k+1)e}$$

induced by f are well-defined and surjective. Since each f_k is also injective and thus bijective, we find, applying Lemma 5.20 to our situation, that f is an isomorphism, and a little reflection shows that it is also a $\mathbb{Z}_p$-module isomorphism. Thus, for $m > e/(p-1)$, U_m is a free $\mathbb{Z}_p$-module of rank n. Since U_1/U_m is finite, this shows that U_1 is a finitely generated $\mathbb{Z}_p$-module, and so by Theorem 1.32 we obtain

$$U_1 \sim \mathbb{Z}_p^t \oplus H$$

with a suitable $t \geq 0$, and a torsion $\mathbb{Z}_p$-module H. Since U_1 contains U_m we have $t \geq n$, and using the finiteness of U_1/U_m we get $t = n$.

Now we show that H is a finite p-group. Since it is finitely generated, and $\mathbb{Z}_p$ has the finite norm property, Theorem 1.41 implies that H is finite, and thus, being a subgroup of the multiplicative group of a field, it consists of roots of unity, hence is cyclic. If H were not a p-group, then it would contain a primitive root of unity u of a prime order $q \neq p$, but Lemma 5.18 implies that H contains u^{1/q^j} for $j = 1, 2, \ldots$, which is not possible, as H is finite. Thus H is a cyclic p-group, i.e. $H \sim C_{p^r}$ with a certain $r \geq 0$, and since H consists of roots of unity, we get $r = s$. □

Corollary. *Let $[K : \mathbb{Q}_p] = n$ and let s be the irregularity index of K. There exist $u_1, \ldots, u_n \in U_1$ such that for fixed $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, every non-zero element of K can be uniquely written in the form*

$$z^a w^b u_1^{m_1} \cdots u_n^{m_n} \pi^N,$$

where $0 \leq a < p^f - 1$, $0 \leq b < p^s$, $m_1, \ldots, m_n \in \mathbb{Z}_p$, z, w are primitive $p^f - 1$-th and p^s-th roots of unity and $N \in \mathbb{Z}$.

Proof: Combine the theorem just proved with Proposition 5.16 and its Corollary 1. □

Because of Proposition 5.13 and Theorem 5.21 we obtain that in the case of a regular field K the $\mathbb{Z}_p$-modules $U_1(K)$, R and $\mathfrak{p}, \mathfrak{p}^2, \ldots$ are all isomorphic. In certain cases it is possible to establish a particular simple isomorphism between $U_1(K)$ and $\mathfrak{p}$. Put $\Omega = \{x \in K : \nu(x) > e/(p-1)\}$ and observe that Ω is a group under addition.

Proposition 5.22. *(i) The series*

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converges for x in Ω and defines a continuous function there.

(ii) The function $\exp x$ provides an isomorphism of Ω onto the multiplicative group $\{x \in K : \nu(x-1) > e/(p-1)\}$.

(iii) If $e < p-1$, then $\exp x$ provides a $\mathbb{Z}_p$-module isomorphism of $\mathfrak{p}$ onto $U_1(K)$.

Proof: We have to show first that for $x \in \Omega$ the general term $x^k/k!$ of our series tends to zero. Now $\nu(x^k/k!) = k\nu(x) - \nu(k!)$, and by elementary number theory $k!$ is divisible exactly by the c_k-th power of p, where

$$c_k = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots + \left[\frac{k}{p^r}\right],$$

and $r \in \mathbb{Z}$ is determined by the inequalities $p^r \leq k < p^{1+r}$. Moreover we have

$$\nu(k!) = ec_k \leq e\left(\frac{k}{p} + \frac{k}{p^2} + \cdots + \frac{k}{p^r}\right) = ek\frac{1-p^{-r}}{p-1} < \frac{ek}{p-1},$$

and since for every $x \in \Omega$ we have $\nu(x) = e(p-1) + \delta$ with $\delta = \delta(x) > 0$, it follows that $\nu(x^k/k!) > \delta k$, thus $\lim_k x^k/k! = 0$. One verifies immediately that for $x, y \in \Omega$ we have $\exp(x+y) = \exp(x)\exp(y)$, and hence exp is indeed a homomorphism. Since the values of $\exp x$ lie in $U_1(K)$ and the continuity at $x = 0$ is evident, (i) results.

Now observe that the minimal value of $\nu(x^k/k!)$ is for non-zero $x \in \Omega$ attained only at $k = 1$. Indeed, if $k\nu(x) - \nu(k!) \leq \nu(x)$ and $k > 1$, then

$$\nu(x) \leq ec_k/(k-1) \leq ek\frac{1-p^{-r}}{(p-1)(k-1)} \leq \frac{e}{p-1},$$

a contradiction. This implies $\nu(\exp x - 1) = \nu(x) > e/(p-1)$, and leads to the injectivity of $\exp x$, since from $x \neq y$ and $\exp x = \exp y$ we obtain $\exp(x-y) = 1$, however $\nu(\exp(x-y) - 1) = \nu(x-y)$, a finite number. To show surjectivity consider the series

$$x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots + (-1)^{n+1}\frac{x^n}{n} + \cdots,$$

which converges for all x satisfying $\nu(x) \geq 1$, and denote its sum by $\log(1+x)$, for obvious reasons. Observe now that if $\nu(y) > e/(p-1)$, then

$$\exp(\log(1+y)) = 1 + y,$$

and so $1 + y$ lies in $\exp(\Omega)$. This proves (ii).

To prove (iii) observe that the assumption $e < p - 1$ and (ii) show that $\exp : \mathfrak{p} \longrightarrow U_1$ is an isomorphism of the additive groups, and it remains to check that exp commutes with the action of $\mathbb{Z}_p$. However, for elements of $\mathbb{Z}$ this follows from the homomorphism property, and the general case results by continuity. □

5.2. Extensions of $\mathfrak{p}$-adic Fields

1. In this section K will be a $\mathfrak{p}$-adic field and L/K an extension of degree $n = ef$, with e being the ramification index of L/K, and f the degree of the residue class field extension k_L/k_K, where k_K and k_L are the residue class fields of K and L, respectively. Denote by p the characteristic of k_K, so that $\mathbb{Q}_p \subset K$. Moreover R and S will denote the rings of integers of K, resp. L

and $\mathfrak{p}$, $\mathfrak{P}$ will be the corresponding prime ideals, whence $\mathfrak{p}S = \mathfrak{P}^e$. By π and Π we shall denote fixed elements from $\mathfrak{p} \setminus \mathfrak{p}^2$ and $\mathfrak{P} \setminus \mathfrak{P}^2$. Finally, ν_K, ν_L will be the corresponding exponents, and v_K, v_L the corresponding valuations, which will be assumed to satisfy

$$v_K(\pi) = p^{-f_{K/\mathbb{Q}_p}}, \quad v_L(\Pi) = p^{-f_{L/\mathbb{Q}_p}}.$$

As before, we shall call the extension L/K *unramified* if $e = 1$, and, moreover, we shall say that it is *totally* (or *fully*) *ramified* if $e = n$, and that it is *tamely ramified* if p does not divide e. An extension which is ramified, but not tamely ramified will be called *wildly ramified*.

We shall first deal with unramified extensions. It will turn out that every $\mathfrak{p}$-adic field has exactly one unramified extension of a given degree, and such extension is necessarily normal with a cyclic Galois group, isomorphic to the Galois group of the corresponding extension of the residue class field. To obtain this we need two lemmas first.

Lemma 5.23. *Let $L = K(\zeta_m)$, where ζ_m denotes a m-th primitive root of unit, and assume that $p \nmid m$. Then the extension L/K is unramified.*

Proof : Let $f \in R[X]$ be the minimal polynomial of ζ_m. Obviously f divides the polynomial $X^m - 1$, and if we write $X^m - 1 = f(X)g(X)$ with $g \in R[X]$, then we obtain that the different of L/K divides $m\zeta_m^{m-1}$, which is a unit of K. The different theorem implies now that L/K is unramified. □

Lemma 5.24. *A finite extension L/K is unramified if and only if there exists $a \in S$ with $L = K(a)$, which has the following property:*

If $F \in R[X]$ is the minimal monic polynomial of a, and $\varphi \in k_K[X]$ is obtained from F be reducing mod $\mathfrak{p}$ *its coefficients, then the image of a in k_L is a simple root of φ.*

Proof : If L/K is unramified, then $n = f = [k_L : k_K]$. Let $\overline{a}$ be a generator of the extension k_L/k_K, denote by $\varphi \in k_K[X]$ its minimal polynomial, and let $F \in R[X]$ be a monic polynomial with $F \bmod \mathfrak{p} = \varphi$. By Corollary 1 to Theorem 5.6 F has a root in L, say a. Moreover F is irreducible over K because of $[L : K] = [k_L : k_K] = [K(a) : K]$, (the last equality resulting from the observation that the residue class field of $K(a)$ equals k_L), thus $L = K(a)$.

To prove the converse, observe first that we can assume the irreducibility of F over K. Corollary 4 to Theorem 5.6 shows that φ is a power of an irreducible polynomial. Thus it must be irreducible itself, since it has a simple root. Hence

$$n = \deg F = \deg \varphi = [k_L : k_K] = f \leq n,$$

and we get $f = n$ and $e = 1$. □

Corollary 1. *If L/K is unramified and $M/\mathbb{Q}_p$ is finite, then LM/KM is unramified.*

Proof : Let $L = K(a)$ with a as in the lemma. Then $LM = KM(a)$, and the image of a in k_{LM} is a simple root of the polynomial φ, minimal for the image of a in k_L over k_K. Therefore the lemma implies that LM/KM is unramified. □

Corollary 2. *If L/K and M/K are unramified, then LM/K is also unramified.*

Proof : Apply the multiplicative property of ramification indices and the preceding corollary. □

Corollary 3. *If L/K is finite, and M is the composite of all unramified extensions of K, contained in L, then M/K is unramified, and L/M is fully ramified. Hence every finite extension can be decomposed into two consecutive extensions: the first unramified and the second fully ramified.*

Proof : By the preceding corollary the extension M/K is unramified. Let $f_1 = [k_L : k_M]$. We may write $k_L = \mathbb{F}_p(\zeta_r)$ with a certain r not divisible by p, ζ_r being a primitive r-th root of unity. Thus the polynomial $X^r - 1$ has r distinct roots in k_L, and so, by Corollary 1 to Theorem 5.6, it has also r roots in L. If we had $f_1 \geq 2$, then not all these roots would lie in M, and so the splitting field N of $X^r - 1$ over K would not be a subfield of M. But we have $N \subset L$, and since Lemma 5.23 and Corollary 2 to Lemma 5.24 show that N/K is unramified, hence $N \subset M$, contradiction. Therefore $f_1 = 1$ and the extension L/M is fully ramified. □

Theorem 5.25. *If K is a $\mathfrak{p}$-adic field, then to every finite extension k/k_K there corresponds a unique unramified extension L/K with $k_L \sim k$. This extension is normal, and its Galois group is isomorphic to the Galois group of k/k_K.*

Proof : Let a be a generator of k/k_K, and let $\varphi \in k_K[X]$ be its minimal polynomial. Choose a monic $F \in R[X]$ with $F \bmod \mathfrak{p} = \varphi$, let b be a root of F lying in a fixed algebraic closure of $\mathbb{Q}_p$, and put $L = K(b)$. Then

$$[L : K] = \deg_K b \leq \deg F = \deg \varphi = [k : k_K] \leq [k_L : k_K] \leq [L : K],$$

because the image of b in k_L is a root of φ, and so $k \subset k_L$. This chain of inequalities shows that $[k_L : k_K] = [L : K]$, thus L/K is unramified, and $[k : k_K] = [k_L : k_K]$, hence $k = k_L$. If L_1/K is another unramified extension with $k_{L_1} = k$, then Hensel's's lemma implies that F has a root $b_1 \in L$, and we have $K(b_1) \sim K(b) = L$. However, in view of $[K(b_1) : K] = [k : k_K] = [L_1 : K]$ we obtain $L_1 = K(b_1)$, and we see that L_1 and L are isomorphic.

Now we shall establish the normality of L/K, and this will force the equality $L_1 = L$. The extension k/k_K is normal, thus k is the splitting field of some polynomial $h \in k_K[X]$. Choose $H \in R[X]$ so that $H \bmod \mathfrak{p} = h$. By Hensel's lemma H splits in L into linear factors, and the preceding argument shows that one of its roots generates L/K, i.e., L is the splitting field of H over K, and we obtain that the extension L/K is normal.

For every $g \in Gal(L/K)$ the formula $\overline{g}(x \bmod \mathfrak{p}) = g(x) \bmod \mathfrak{p}$ defines an automorphism $\overline{g} \in Gal(k/k_K)$. The map $\Psi : g \mapsto \overline{g}$ is obviously a homomorphism, and we shall now show that it is bijective. Since the Galois groups of L/K and k/k_K have the same number of elements, it suffices to prove that Ψ is surjective. Let b, φ and F have the same meaning as at the beginning of the proof, and put $a = b \bmod \mathfrak{p}$. If $\sigma \in Gal(k_K/k)$, then $\sigma(a) = a_1$ is a root of φ, and Hensel's lemma implies the existence of $b_1 \in S$ such that $F(b_1) = 0$, and $b_1 \bmod \mathfrak{p} = a_1$. Such element b_1 is unique, because φ has in k as many roots as F has in L, and so all roots of F have distinct images in k. If now $g \in Gal(L/K)$ takes b into b_1, then $\Psi(g) = \sigma$, proving the surjectivity of Ψ. □

Corollary 1. *Every $\mathfrak{p}$-adic field has exactly one unramified extension of a given degree.*

Proof : There is exactly one extension of a given degree of the finite field k_K. □

Corollary 2. *If L/K is unramified, then its Galois group is cyclic.*

Proof : Every finite extension of a finite field is cyclic. □

To conclude the subsection devoted to unramified extensions we give an explicit description of them.

Theorem 5.26. *If K is a $\mathfrak{p}$-adic field, then its finite extension L/K is unramified if and only if $L = K(\zeta_m)$, where ζ_m is a primitive m-th root of unity, with $p \nmid m$.*

Proof : The sufficiency is contained in Lemma 5.23. To prove the necessity assume that L/K is unramified. If we put $f = f(L/\mathbb{Q}_p)$, then we obtain that the field k_L has p^f elements, and its multiplicative group is cyclic of order $m = p^f - 1$. Therefore its generator equals ζ_m, and we get $k_L = k_K(\zeta_m)$. Applying Hensel's lemma we see that all m-th roots of unity lie in L. If L_1/K is generated by a primitive m-th rot of unity, then L_1 has the same residue class field as L, whence, since L/L_1 is unramified, we obtain $L = L_1$. □

Corollary. *If $L = K(\zeta_m)$ and $p \nmid m$, then every subfield of L, containing K is of the form $K(\zeta_r)$, with r not divisible by p.*

Proof : Every subfield of a field unramified over K is also unramified. □

2. Now we turn to fully ramified extensions L/K, in which case $f(L/K) = 1$. We shall show that every such extension can be generated over K by a root of an Eisensteinian polynomial, i.e., a monic polynomial whose coefficients, except the leading one, lie in the prime ideal $\mathfrak{p}$ of R, and the free term does not lie in $\mathfrak{p}^2$. In the same way as in the rational case one shows that every such polynomial is irreducible over K.

Theorem 5.27. *If K is a $\mathfrak{p}$-adic field, and the extension L/K is fully ramified, then there exists an Eisensteinian polynomial over K, whose root a generates L/K, and, moreover, $S = R[a]$. Conversely, every extension generated by a root of an Eisensteinian polynomial is fully ramified.*

Proof : Let L/K be fully ramified. We can use Theorem 5.2 with the set A of representatives of S mod $\mathfrak{P}$, contained in R, to get the existence of $a \in \mathfrak{P} \setminus \mathfrak{P}^2$ with $S = R[a]$. Indeed, it suffices to choose $b \in R$ with $\nu_K(b) = 1$, and to define $t_k = b^i a^j$ for $k = ie + j$ with $j = 0, 1, \ldots, e-1$. Let $F(X) = X^e + \sum_{j=0}^{e-1} c_j X^j$ be the minimal polynomial of a over R. Since $a^e + \sum_{j=0}^{e-1} c_j a^j = 0$ we see that $c_0 \in \mathfrak{p}$, thus $\nu_L(c_0) \geq 1$. Assume now that $c_0, c_1, \ldots, c_{j-1}$ all lie in $\mathfrak{p}$. Thus $c_i = bb_i$ with $b_i \in R$, and

$$-c_j a^j = a^e + \cdots + c_{j+1} a^{j+1} + b(b_{j-1} a^{j-1} + \cdots + b_0),$$

and in view of $a^e | b$ we see that c_j is divisible by a, hence lies in $\mathfrak{p}$. It follows by induction that all c_j's lie in $\mathfrak{p}$. Moreover $\nu_L(a^e) = e$, and for $j = 1, 2, \ldots, e-1$ we have $\nu_L(c_j a^j) > e$, hence $\nu_L(c_0) = e$, leading to $\nu_K(c_0) = 1$, which shows that F is indeed Eisensteinian.

To prove the converse assume that L/K is generated by a root a of an Eisensteinian polynomial $X^n + \sum_{j=0}^{n-1} c_j X^j$. Obviously $\nu_L(a^n)$ is positive, thus $\nu_L(a) \geq 1$. This shows that

$$n\nu_L(a) = \nu_L(a^n) = \nu_L(c_0) = e,$$

whence n cannot exceed e, and finally $n = e$, showing that L/K is fully ramified. □

Corollary 1. *Every $\mathfrak{p}$-adic field has fully ramified extensions of any prescribed degree.*

Proof : In fact, the field generated over K by any root of the polynomial $X^n + \pi$ is fully ramified over K. □

Corollary 2. *A $\mathfrak{p}$-adic field has only finitely many extensions of given degree.*

Proof : Let K be a $\mathfrak{p}$-adic field and fix a positive integer n. If L/K is an extension of degree n, and M/K is the maximal unramified extension of K contained in L, then it follows from Corollary 1 to Theorem 5.25 that we have only finitely many possibilities for M, since $[M : K]$ is a divisor of n. Corollary 3 to Lemma 5.24 shows that it suffices now to prove that each such field M has only finitely many fully ramified extensions of a given degree m, because the degree of L/M divides n. To obtain that, let $\mathfrak{p}$ be the prime ideal of the ring of integers R of M, let X be the Cartesian product of $m-1$ copies of $\mathfrak{p}$, and consider

$$\Omega = X \times (\mathfrak{p} \setminus \mathfrak{p}^2)$$

with the product topology. Since $\mathfrak{p}$ as well as $\mathfrak{p}^2$ are both compact and open, we see that Ω is compact. For a monic Eisensteinian polynomial $f = X^m + \sum_{j=0}^{m-1} a_j X^j \in R[X]$ denote by $\Psi(f)$ the element $[a_{m-1}, \ldots, a_0]$ of Ω, and observe that the map Ψ is one-to-one. For a given fully ramified extension N/M let V_N be the set of all Eisensteinian polynomials whose roots include a generator of N/M. Proposition 5.9 implies that the set $f(V_N)$ is an open subset of Ω, and since the theorem shows that their union covers Ω, we infer from the compactness of Ω that there is a finite subcovering, and this means that roots of Eisensteinian polynomials of degree m generate a finite number of extensions of M. □

Note that the composition of two fully ramified extensions may not be fully ramified, as the following example shows:

Take $K = \mathbb{Q}_3$, $K_1 = K(\sqrt{3})$, $K_2 = K(\sqrt{-3})$ and $L = K_1 K_2$. The extensions K_i/K $(i = 1, 2)$ are fully ramified by the preceding theorem with $e(K_i/K) = 2$. Since -1 is not a square mod 3, it cannot be a square in $\mathbb{Q}_3$, hence $K_1 \neq K_2$. In view of Theorem 5.26 the extension L/K_1 is unramified, as $L = K_1(\sqrt{-1})$, and so we get $e(L/K) = e(L/K_1)e(K_1/K) = 2$. As $[L : K] = 4$ we obtain $f(L/K) = 2$, showing that L/K is not fully ramified.

Now we shall use Theorem 5.27 and Corollary 3 to Lemma 5.24 to obtain a refinement of the different theorem for $\mathfrak{p}$-adic fields, which will be extended in Chap. 6 to algebraic number fields.

Proposition 5.28. *If K is a $\mathfrak{p}$-adic field and the extension L/K is wildly ramified, i.e., $\mathfrak{p}|e$, then the different $D_{L/K}$ is divisible by $\mathfrak{P}^e$.*

Proof : By Corollary 3 to Lemma 5.24 we can assume that L/K is fully ramified. Choose Π in S in such a way that $S = R[\Pi]$, $\nu_L(\Pi) = 1$, and the minimal polynomial $f(X) = X^e + \sum_{j=0}^{e-1} a_j X^j \in R[X]$ of Π is Eisensteinian. Then we have

$$\nu_L(f'(\Pi)) = \nu_L(e\Pi^{e-1} + \sum_{j=1}^{e-1} j a_j \Pi^{j-1})$$
$$\geq \min\{\nu_L(e\Pi^{e-1}), \nu_L(a_1), \nu_L(2a_2\Pi), \ldots, \nu_L((e-1)a_{e-1}\Pi^{e-2})\},$$

and since $\nu_L(e\Pi^{e-1}) = \nu_L(e) + e - 1 \geq e$, and for every $j = 1, 2, \ldots, e-1$ we have $\nu_L(j a_j \Pi^{j-1}) \geq \nu_L(a_j) + j - 1 \geq e + j - 1 \geq e$, we obtain $\nu_L(f'(\Pi)) \geq e$, and so $D_{L/K} = f'(\Pi)S$ is divisible by $\mathfrak{P}^e$. □

Corollary. *If K is a $\mathfrak{p}$-adic field and $[L : K] = n$, then the following conditions are equivalent:*
(i) L/K is tame,
(ii) $\mathfrak{p}^n \nmid d(L/K)$,
(iii) $T_{L/K}(S) = R$.

Proof : The equivalence of (i) and (ii) results from Theorem 4.24 and the proposition just proved. To prove the equivalence of (i) and (iii) we use Corollary 3 to Proposition 4.13, according to which (iii) holds if and only if $D_{L/K}$ has no divisors of the form AS with A being a proper ideal of R. Since $D_{L/K} = \mathfrak{P}^m$ with $m \leq e - 1$ if L/K is tame, and $m \geq e$ otherwise (by Theorem 4.24 and the above proposition), and $\mathfrak{P}^e$ is the minimal power of $\mathfrak{P}$ of the form AS with $A \subset R$, $A \neq R$, the assertion follows. □

3. Now we shall look at tame extensions. Since every such extension can be decomposed in two consecutive extensions – the first unramified, and the second fully and tamely ramified (Corollary 3 to Lemma 5.24), and since we already know the structure of unramified extensions, we may restrict our attention to fully ramified tame extensions.

Theorem 5.29. *If K is a $\mathfrak{p}$-adic field, then the extension L/K is fully and tamely ramified if and only if $L = K(a)$, where $a \in S$ is a root of $X^n - b$ with $\nu_K(b) = 1$ and $p \nmid n$.*

Proof : The sufficiency of the condition stated results from Theorem 5.27 and the observation that in this case we have $e(L/K) = n$, and $p \nmid n$. To prove its necessity we need a lemma:

Lemma 5.30. *Let L/K be a finite extension of a $\mathfrak{p}$-adic field K, $p \nmid m$ and $a \in R$. If $b \in S$ satisfies $\nu_L(b^m) = \nu_L(a)$, and the quotient b^m/a is congruent* mod $\mathfrak{P}$ *to a unit of K, then there exists $c \in R$, differing from a at most by a unit factor, such that the polynomial $X^m - c$ has a root in $K(b) \subset L$.*

Proof : If $b^m/a \equiv \epsilon \pmod{\mathfrak{P}}$, with $\epsilon \in U(K)$, then put $c = \epsilon a$. If $x_1, \ldots, x_m$ are all roots of $f(X) = X^m - c$ in a fixed algebraic closure of L, and v is the extension of the valuation of L to the splitting field of f, then we have

$$\prod_{i=1}^{m} v(b-x_i) = v(b^m - c) = v(a)v(b^m/a - c/a)$$
$$= v(a)v(b^m/a - \epsilon) < v(a) = v(b)^m,$$

thus for a certain j we have $v(b-x_j) < v(b)$, and therefore $v(b) = v(x_j)$. Moreover

$$v(b)^{m-1} = v(x_j)^{m-1} = v(f'(x_j)) = \prod_{i \neq j} v(x_i - x_j),$$

but for $i \neq j$ we have $v(x_i - x_j) \leq \max\{v(x_i), v(x_j)\} = v(b)$, hence for $i \neq j$ we should have $v(x_i - x_j) = v(b)$. Finally, we obtain for $i \neq j$ the inequality $v(b - x_j) < v(x_i - x_j)$, and we may apply Proposition 5.8. □

Now assume that L/K is fully and tamely ramified of degree $n = e$. With a suitable unit $\epsilon \in L$ we have $\pi = \epsilon \Pi^e$. Since in our case $f = 1$, we can find a unit η in K congruent to ϵ mod $\mathfrak{P}$. Applying Lemma 5.30 with $m = e$, $a = \pi$, $b = \Pi$, we obtain the existence of $c \in K$ with $\nu_K(c) = 1$ such that the polynomial $X^e - c$ has in L a root, say x_0. Since this polynomial is Eisensteinian, it is irreducible, hence $[K(x_0) : K] = e$, and we get $K(x_0) = L$. □

Corollary 1. *If L/K is tame and M/K is finite, then the extension LM/M is tame.*

Proof : Let L_0 be the maximal unramified extension of K contained in L. The extension L/L_0 is fully and tamely ramified, hence by Theorems 5.26 and 5.29 we have $L = L_0(a)$, $L_0 = K(\zeta_r)$, where a is a root of $X^m - b$ with some $b \in L_0$, satisfying $\nu_{L_0}(b) = 1$, $p \nmid m = e(L/L_0) = e(L/K)$ and $p \nmid r$. Put $M_1 = M(\zeta_r, \zeta_m)$ and $N_1 = M_1(a)$. Lemma 5.23 and Corollary 2 to Lemma 5.24 imply that M_1/M is unramified. Since $LM \subset N_1 = M_1(a)$ it suffices to show that N_1/M is tame. Since M_1 contains all m-th roots of unity we can write

$$X^m - b = \prod_{j=0}^{m-1} (X - \zeta_m^j a),$$

and if $f(X) = \prod_{j \in J}(X - \zeta_m^j a)$ is a factor of $X^m - b$, irreducible over M_1 (with $J \subset \{0, 1, \ldots, m-1\}$), then with $s = \#J$ we get $a^s \in M_1$. Choose now such a factor f with the minimal possible value of s, and observe that s divides m. If $b_1 = a^s$, then $f(X) = X^s - b_1$. Indeed, $X^s - b_1$ is divisible by f, because f is irreducible and has a common root with $X^s - b_1$, and now the equality of degrees implies the equality of polynomials.

Finally, since N_1/M_1 is fully ramified, we obtain $e(N_1/M_1) = [N_1 : M_1] = s | m$, but $p \nmid m$, and thus N_1/M_1 is tame. □

Corollary 2. *If L/K and M/K are both tame, then so is LM/K.*

Proof : Apply Corollary 1 and the multiplicativity of ramification indices at consecutive extensions. □

Corollary 3. *If L/K is finite and M is the composite of all tame extensions of K contained in L, then M/K is tame, and if $M \neq L$, then L/M is a wildly and fully ramified extension, whose degree is a power of p. We have thus $e(L/K) = e_1 p^k$ with $p \nmid e_1 = e(M/K)$ and $p^k = [L : M]$.*

Proof : The tameness of M/K results from Corollary 2. If $M = L$, then there is nothing more to prove. Assume thus $M \neq L$. Since M is the maximal tame extension of K contained in L, the extension L/M must be wildly and fully ramified. Put $e_1 = e(L/M)$ and write $[L : M] = e_1 = e_0 p^k$ with a certain e_0 not divisible by p. Applying Lemma 5.30 for $m = e_0$, $a = \pi_M$, $b = \pi_L^{p^k}$ (where π_L, π_M generate the prime ideals in the rings of integers of L and M, respectively), we obtain that with a suitable unit $\epsilon \in M$ the polynomial $X^{e_0} - \epsilon\pi_M$ has a root $\xi \in L$. Theorem 5.29 implies that the extension $M(\xi)/M$ is tame, and therefore $\xi \in M$. Thus $e_0 = 1$. □

Corollary 4. (Abhyankar's lemma) *If L/K is tame, M/K is finite and $e(L/K)$ divides $e(M/K)$, then LM/M is unramified.*

Proof : Let L_0 be the maximal subfield of L, unramified over K. By Corollary 3 to Lemma 5.24 the extension L/L_0 is fully ramified. Since Corollary 1 to that lemma implies that L_0M/M is unramified, we get $e(L_0M/K) = e(M/K)$, and this leads to

$$e(M/K) = e(L_0M/K) = e(L_0M/L_0)e(L_0/K) = e(L_0M/L_0).$$

Since L/L_0 is fully and tamely ramified, Theorem 5.29 shows that we may write $L = L_0(\pi)$ where π is a root of a polynomial $X^e - a$, with $e = e(L/K)$, $a \in L_0$ and $\nu_{L_0}(a) = 1$. If $b \in L_0M$ satisfies $\nu_{L_0M}(b) = 1$, then with a certain unit u of L_0M we have $a = ub^{e(M/K)}$. Since $e | e(M/K)$ we get, with $e' = e(M/K)/e$, the equality $\pi^e = ub^{ee'}$, thus $(\pi b^{-e'})^e = u$, leading to $LM = L_0M(u^{1/e})$.

Using Proposition 5.16 we can write $u = \zeta u_1$, with a root of unity ζ of order not divisible by p, and $u_1 \in U_1(L_0M)$. Because of $p \nmid e$ the number $1/e$ is a p-adic integer, thus Theorem 5.21 gives $u_1^{1/e} \in L_0M$. Hence $LM = L_0M(\xi)$, where ξ is a root of unity of order not divisible by p. Now we may invoke Theorem 5.26 to obtain that LM/L_0M is unramified. Finally, we arrive at

$$e(LM/M) = e(LM/L_0M)e(L_0M/M) = 1,$$

and thus LM/M is unramified, as asserted. □

4. In this subsection we give some examples. First we enumerate quadratic extensions of a given $\mathfrak{p}$-adic field.

Proposition 5.31. *Let K be a $\mathfrak{p}$-adic field of degree n over $\mathbb{Q}_p$, put $f = f(K/\mathbb{Q}_p)$, and let π be a fixed generator of the prime ideal of the ring of integers of K.*

(i) If $p \neq 2$, then K has three quadratic extensions, namely $K(\sqrt{\pi})$, $K(\sqrt{\zeta\pi})$ and $K(\sqrt{\zeta})$, where ζ is the primitive root of unity of order $p^f - 1$.

(ii) If $p = 2$, then K has $2^{n+2} - 1$ quadratic extensions, each of them of the form $K(\sqrt{a})$ or $K(\sqrt{a\pi})$ with

$$a = \zeta^{a_0}\epsilon_1^{a_1}\cdots\epsilon_n^{a_n}, \tag{5.6}$$

where ζ is the primitive 2^s-th root of unity, s is the irregularity index of K, $\epsilon_1, \ldots, \epsilon_n$ are the free generators of the free summand of $U_1(K)$, as described in Theorem 5.21, and $a_i \in \{0, 1\}$ $(i = 0, 1, \ldots, n)$.

(iii) In both cases exactly one extension is unramified and all others are fully ramified (in case (i) tamely, and in case (ii) wildly).

Proof : Note that for any field K of characteristic $\neq 2$ the quadratic extensions are in a one-to-one correspondence with elements of $K^*/(K^*)^2$, where $(K^*)^2$ is the group of all non-zero squares of elements of K. Indeed, every quadratic extension of K is of the form $K(\sqrt{a})$ with $a \in K \setminus (K^*)^2$, and if $a, b \in K^*$ lie in the same coset mod $(K^*)^2$, then $a = bc^2$ holds with $c \in K^*$, thus $K(\sqrt{a}) = K(\sqrt{b})$. Conversely, if $K(\sqrt{a}) = K(\sqrt{b})$, then $\sqrt{a} = A + B\sqrt{b}$ holds with $A, B \in K$, and a short computation shows that a and b lie in the same coset mod $(K^*)^2$.

Proposition 5.16 and its Corollary 1 force us to look at the factor groups $E_1(K)/E_1(K)^2$, $U_1(K)/U_1(K)^2$ and $\mathbb{Z}/2\mathbb{Z}$. The last group being trivially cyclic of order two, we are left with the first two. Assume first $p \neq 2$. Then $U_1(K) = U_1(K)^2$, since $1/2$ is an integral element of $\mathbb{Q}_p$, hence every principal unit is a square of a principal unit. Since $E_1(K)$ is cyclic of even order $p^f - 1$, thus $E_1(K)/E_1(K)^2$ is of order two, and finally we get $K^*/(K^*)^2 \sim C_2 \times C_2$. The representatives of the cosets may be taken to be equal to 1, ζ, π and $\zeta\pi$, and this gives us three quadratic extensions of K, the first of which is unramified and the others fully and tamely ramified.

Now let $p = 2$. In this case $E_1(K)$ is a cyclic group of odd order, and hence every its element is a square. By Theorem 5.21 we can write every element $u \in U_1(K)$ in the form

$$u = \zeta^{c_0}\epsilon_1^{c_1}\cdots\epsilon_n^{c_n},$$

with $0 \leq c_0 < 2^s$, and $c_1, \ldots, c_n \in \mathbb{Z}_p$. Writing each c_i in the form $c_i = a_i + 2b_i$ with $a_i = 0, 1$ and $b_i \in \mathbb{Z}_p$ we get

$$u = \zeta^{a_0}\epsilon_1^{a_1}\cdots\epsilon_n^{a_n}\epsilon^2,$$

with $\epsilon \in U_1(K)$. Thus every coset of $U_1(K)$ mod $U_1(K)^2$ contains an element of the form (5.6), and one sees easily that they all lie in distinct cosets. Thus there are 2^{1+n} such cosets, hence $K^*/(K^*)^2 \sim C_2^{n+2}$, as asserted. The remaining assertions are now immediate. □

In the case $K = \mathbb{Q}_2$ we can be more explicit. Proposition 5.31 shows that $\mathbb{Q}_2$ has 7 quadratic extensions. Observe now that $\mathbb{Q}_2$ does not contain a fourth primitive root of unity, because the congruence $X^2 + 1 \equiv 0 \,(\mathrm{mod}\, 4)$ has no solutions, so $s = 1$ and $\zeta = -1$. Moreover 2 generates the prime ideal, hence to find the generators of quadratic extensions one has to determine the generator ϵ_1 of the free summand of $U_1(\mathbb{Q}_2)$. To find it observe that the proof of Theorem 5.21 shows that ϵ_1 generates the cyclic group U_2/U_3, because in our case the Corollary to Lemma 5.19 applies from $m = 2$ on. Since $U_2/U_3 \sim C_2$, we can take for ϵ_1 any element of $U_2 \setminus U_3$, for example $\epsilon_1 = 5$. It follows that $\mathbb{Q}_2$ has the following quadratic extensions: $\mathbb{Q}_2(\sqrt{5})$, $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-5})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{10})$ and $\mathbb{Q}_2(\sqrt{-10})$. Since the congruence $X^2 \equiv 5 \,(\mathrm{mod}\, 4)$ is solvable, Corollary to Theorem 5.15 shows that $\mathbb{Q}_2(\sqrt{5})$ is the only unramified quadratic extension of $\mathbb{Q}_2$, the remaining being fully and wildly ramified.

Now consider biquadratic extensions, i.e. normal quartic extensions with Galois group isomorphic to $C_2 \oplus C_2$.

Proposition 5.32. *Let $K/\mathbb{Q}_p$ be an extension of degree n, and let ζ and π have the same meaning as in the preceding proposition.*

(i) If $p \neq 2$, then K has exactly one biquadratic extension, namely $L = K(\sqrt{\pi}, \sqrt{\zeta})$. One has $e(L/K) = f(L/K) = 2$, thus L/K is ramified and tame.

(ii) If $p = 2$, then every biquadratic extension of K equals $K(\sqrt{a}, \sqrt{b})$, with a, b of the form given in (5.6). *Not all such extensions are distinct, and all possible equalities between them are of the form*

$$K(\sqrt{a}, \sqrt{b}) = K(\sqrt{a}, \sqrt{c}) = K(\sqrt{b}, \sqrt{c}),$$

with $abc^{-1} \in (K^*)^2$. All these extensions are wildly ramified. If one of the fields $K(\sqrt{a})$, $K(\sqrt{b})$, $K(\sqrt{c})$ is unramified over K, then for $L = K(\sqrt{a}, \sqrt{b})$ we have $e(L/K) = f(L/K) = 2$. In all other cases $e(L/K) = 4$, $f(L/K) = 1$, thus L/K is fully ramified.

Proof : (i) Since a biquadratic extensions contains three quadratic subfields, the preceding proposition implies $L = K(\sqrt{\pi}, \sqrt{\zeta})$. As L contains $K(\sqrt{\zeta})$, which is unramified over K, we have $e(L/K) \leq 2$. On the other hand $K(\sqrt{\pi}) \subset L$ is ramified, whence $e(L/K) = 2$, and $f(L/K) = 2$ follows.

(ii) The assertions are immediate — it suffices to observe that none of the extensions $K(\sqrt{a}, \sqrt{b})/K$ can be unramified, since the Galois group is not cyclic, and if a field does not contain an unramified subextension $\neq K$, then it has to be fully ramified. □

Corollary. *If K is an extension of $\mathbb{Q}_p$ with odd p, then there is no Galois extension of K with Galois group C_2^N with $N \geq 3$.*

Proof : If such extension would exist, then K would have at least two biquadratic extensions, contradicting part (i) of the proposition. □

5. Now we shall consider normal extensions of $\mathfrak{p}$-adic fields. Our notation will be the same as in previous subsections.

We shall define a sequence of subgroups of $G = Gal(L/K)$, the study of which leads to important results concerning the structure of finite extensions of $\mathfrak{p}$-adic fields, and, as we shall see in the next chapter, also of algebraic number fields.

First we define a map of G onto $Gal(k_L/k_K)$. Let $g \in G$ and $a \in S$. Then the element $\overline{g(a)}$ (where by $\overline{x}$ we denote the canonical image of elements of S and R in k_L and k_K, respectively) depends only on $\overline{a}$. Indeed, if $\overline{a} = \overline{b}$, then $\nu_L(a-b) \geq 1$ and thus $\nu_L(g(a)-g(b)) \geq 1$ and $\overline{g(a)} = \overline{g(b)}$. If we now define the map $\overline{g}: \ \overline{a} \mapsto \overline{g(a)}$ of k_L into k_L, then one sees immediately that it is an automorphism of k_L, leaving k_K fixed, and hence belonging to $Gal(k_L/k_K)$.

Proposition 5.33. *The map $\Phi : g \mapsto \overline{g}$ is a homomorphism of $G = Gal(L/K)$ onto $Gal(k_L/k_K)$, whose kernel G_0 consists of all those $g \in G$ for which the congruence $g(y) \equiv y \pmod{\mathfrak{P}}$ holds for all $y \in S$.*

Proof : The surjectivity of Φ was established in the last part of the proof of Theorem 5.25, where the assumption that L/K is unramified was not used. The remaining assertions are clear. □

The group G_0 occurring in the last proposition is called the *inertia group* of the extension L/K. Now we define for $i = 1, 2, \ldots$ the *ramification groups* G_i of L/K by

$$G_i = \{g \in G_0 : \ g(x) - x \in \mathfrak{P}^{i+1} \text{ for all } x \in S\}.$$

Let us check that the G_i's are indeed groups. Take $g_1, g_2 \in G_i$ and let $x \in S$. Then

$$(g_1 g_2)(x) - x = g_1(g_2(x)) - g_2(x) + g_2(x) - x \in \mathfrak{P}^{i+1},$$

hence $g_1 g_2 \in G_i$, and since G_i is finite, it is a group.

Note that for i sufficiently large the i-th ramification group is trivial, since an element lying in all G_i's has to satisfy $g(x) - x \in \mathfrak{P}^i$ for every non-zero $x \in S$ and all i, and this can happen only if g is the identity. The last non-trivial ramification group will be denoted by G_t.

The next theorem gives the main properties of the sequence $G_0, G_1, \ldots$.

Theorem 5.34. *Let L/K be a normal extension of a $\mathfrak{p}$-adic field K and let G be its Galois group.*

(i) The maximal unramified extension L_0/K contained in L corresponds by Galois theory to the inertia group G_0 of L/K. The inertia group is a normal subgroup of G of order $e(L/K)$, and the factor group G/G_0 is cyclic of order $f(L/K)$. If we identify the groups G_0 and $Gal(L/L_0)$, then the ramification groups of L/K and L/L_0 coincide.

(ii) The maximal tamely ramified extension L_1/K contained in L corresponds by Galois theory to the first ramification group G_1 of L/K. The group G_1 is a normal subgroup of G; it is a p-group, and the factor-group G_0/G_1 is cyclic of order not divisible by p. Moreover, there exists an embedding of G_0/G_1 into the multiplicative group of k_L.

(iii) For $i = 1, 2, \ldots, t$ the ramification groups G_i are normal subgroups of G, and the factor-group G_i/G_{i+1} can be isomorphically embedded in U_i/U_{i+1}. These isomorphisms are induced by the maps $f_i : G_i \longrightarrow U_i/U_{i+1}$, defined by

$$f_i(g) = g(\Pi)\Pi^{-1} \pmod{\mathfrak{P}^i}.$$

Proof: The group corresponding to L_0 can be identified with $Gal(L/L_0)$. Let $g \in Gal(L/L_0)$. As every element of k_L has a representative in L_0, which is invariant under g, we get $g \in G_0$, thus $Gal(L/L_0) \subset G_0$. To prove that these groups are equal it remains to show that they are of the same order. The isomorphism $Gal(L_0/K) \sim G/Gal(L/L_0)$ shows that

$$\#Gal(L/L_0)\#Gal(L_0/K) = \#G,$$

but, on the other hand, Theorem 5.25 and Proposition 5.33 give

$$G/G_0 \sim Gal(k_L/k_K) \sim Gal(L_0/K),$$

whence $\#G_0 = \#G/\#Gal(L_0/K)$, and this implies $G_0 = Gal(L/L_0)$. Since G/G_0 is equal to the Galois group of a unramified extension, it is cyclic by Corollary 2 to Theorem 5.25. The statements about the order become now evident, and the last assertion follows from the fact that G_0 leaves L_0 invariant.

(ii) Consider the map $\Phi : G_0 \longrightarrow k_L^*$ defined by

$$\Phi(g) = g(\Pi)\Pi^{-1} \bmod \mathfrak{P}.$$

This map does not depend on the choice of Π, since for every unit ϵ of L we have

$$g(\epsilon\Pi)(\epsilon\Pi)^{-1} \equiv g(\epsilon)\epsilon^{-1}g(\Pi)\Pi^{-1} \equiv g(\Pi)\Pi^{-1} \bmod \mathfrak{P},$$

in view of $g(\epsilon)\epsilon^{-1} \equiv 1 \pmod{\mathfrak{P}}$ for $g \in G_0$. Moreover Φ is a homomorphism, since

$$\Phi(gh) = g(h(\Pi))\Pi^{-1} \bmod \mathfrak{P} = g(h(\Pi))h(\Pi)^{-1}h(\Pi)\Pi^{-1} \bmod \mathfrak{P}$$
$$= \Phi(g)\Phi(h)$$

holds in view of $h(\Pi) = \epsilon\Pi$, with a unit ϵ. It is clear that the kernel of Φ equals G_1. If e_1 is the order of the image of Φ, then $p \nmid e_1$, and if M is the field corresponding to G_1, then $G_1 \subset G_0$ shows that M contains L_0, which is the maximal unramified extension of K contained in L. Moreover we have $[L : M] = \#G_1 = e(L/K)/e_1$, and since L/M is fully ramified, because of $L_0 \subset M$, we obtain $e_1 = e(L/K)/e(L/M) = e(M/K)$, hence M/K is tame, i.e., $M \subset L_1$. We now have the following situation

$$K \underset{f}{\subset} L_0 \underset{e_1}{\subset} M \underset{e_2}{\subset} L_1 \underset{p^k}{\subset} L,$$

where the subscripts indicate the respective degrees, $e(L/K) = e_0 p^k$ with $p \nmid e_0$ and $e_2 = e_0/e_1$.

Observe now that $Gal(L/L_1)$ is the unique maximal p-subgroup of the group $Gal(L/M)$. Indeed, if $Gal(L/M)$ would have another maximal p-subgroup, then we could take the corresponding field, and compose it with L_1 to get a tame extension of K larger than L_1, and contained in L. Therefore $Gal(L/L_1)$ is a normal subgroup of $Gal(L/M)$, and this shows that L_1/M is normal, tame and fully ramified. By Theorem 5.29 we can write $L_1 = M(a)$ with integral a, generating the prime ideal in the ring of integers of L_1, and satisfying $a^{e_2} = b \in M$. If $g \in G_1$, then we can write $g(a) - a = A\Pi^2$ with $A \in S$, and this gives

$$a^{e_2} = b = g(b) = g(a^{e_2}) = g(a)^{e_2} = (a + A\Pi^2)^{e_2},$$

hence $1 = u^{e_2}$, with

$$u = 1 + \frac{A\Pi^2}{a}.$$

Observe that u is a principal unit of L. Since $p \nmid e_2$, we have $1/e_2 \in \mathbb{Z}_p$, therefore elements of $U_1(L)$ have unique e_2-th roots, so $u = 1$, and we get $g(a) = a$. Thus g leaves L_1 invariant, hence $L_1 = M$ results.

Since all conjugates to L_1 are equal L_1 we see that G_1 is normal. The map Φ induces an embedding of G_0/G_1 into the cyclic group k_L^*, and this implies that G_0/G_1 is cyclic itself.

(iii) It suffices to check that all maps f_i are homomorphisms independent of the choice of Π, and this can be accomplished in the same way as in (ii). The equality Ker $f_i = G_{i+1}$ is evident. To obtain the normality of G_i in G note that G_i is the maximal subgroup of G acting trivially on the quotient $S/\mathfrak{P}^{i+1}$, and it is clear that if g lies in G and h acts trivially on $S/\mathfrak{P}^{i+1}$, then ghg^{-1} does the same. □

Corollary 1. *If $F = f(L/\mathbb{Q}_p)$, then for $i = 1, 2, \ldots, t$ the quotients G_i/G_{i+1} are embeddable in the group C_p^F.*

Proof : Follows from (iii) and the Corollary to Proposition 5.17. □

Corollary 2. *Let L_i be the field corresponding by Galois theory to the group G_i $(i = 0, 1, \ldots, t)$. Then $K \subset L_0 \subset \ldots \subset L_t \subset L$, and if we write $e(L/K) = e_0 p^k$ with $p \nmid e_0$, then $e(L_0/K) = 1$, $e(L_1/L_0) = e_0$, and for $i = 1, 2, \ldots, t$ we have $e(L_{i+1}/L_i) = p^{a_i}$ with a_i positive, except the case when $L_{i+1} = L_i$. Moreover we have $e(L/L_t) = p^{a_t}$ with positive a_t, $a_1 + a_2 + \cdots + a_t = k$, $f(L_0/K) = f(L/K)$ and $f(L/L_0) = 1$. The extensions L_0/K and L_1/L_0 are cyclic and $Gal(L/L_1)$ is a p-group.*

Proof : This is an immediate consequence of the theorem. □

Corollary 3. *The Galois group of any finite normal extension of a $\mathfrak{p}$-adic field is solvable.*

Proof : By Corollary 2 every such extension can be obtained in three consecutive steps: first two cyclic extensions, and then an extension, whose Galois group is a p-group. Since at every step we have a solvable group the assertion results. □

Now we can determine the different of a normal extension in terms of its ramification groups. Before doing this, we prove a simple lemma allowing us to determine whether a given element of G_0 belongs to the i-th ramification group.

Lemma 5.35. *If $S = R[a]$, then the element $g \in G_0$ lies in G_i if and only if*

$$\nu_L(g(a) - a) \geq 1 + i.$$

Proof : The necessity of this condition being evident, we turn to its sufficiency. Write a non-zero element $x \in S$ in the form $x = c_0 + c_1 a + \cdots + c_{n-1} a^{n-1}$ with $c_i \in R$. Then

$$g(x) = c_0 + c_1 g(a) + \cdots + c_{n-1} g(a)^{n-1} \equiv x \pmod{\mathfrak{P}^{i+1}},$$

and since $g(a) - a$ divides $g(x) - x$, our assertion follows. □

Corollary. *If $S = R[a]$, then for $i = 0, 1, \ldots, t$ we have*

$$G_i \setminus G_{i+1} = \{g : \ \nu(g(a) - a) = i + 1\}.$$

Proof : Clear. □

Now we can obtain a formula for the different of a normal extension:

Theorem 5.36. *If L/K is normal, then $D_{L/K} = \mathfrak{P}^A$, where*

$$A = \sum_{j=0}^{t} (\#G_j - 1)\,.$$

Proof : In view of Theorems 4.24 and 5.34 (i) it suffices to prove this formula for fully ramified extensions. Assume thus that L/K is fully ramified. Then by Theorem 5.27 we have $S = R[a]$ for some a with $\nu_L(a) = 1$. If $f \in R[X]$ is the minimal polynomial of a, then $D_{L/K} = f'(a)S$, hence $A = \nu_L(f'(a))$. Since

$$f'(a) = \prod_{g \in G, g \neq e} (a - g(a)),$$

and in our case $G = G_0$, thus

$$\begin{aligned}\nu_L(f'(a)) &= \sum_{\substack{g \in G \\ g \neq e}} \nu_L(a - g(a)) \\ &= \sum_{j=0}^{t-1} \sum_{g \in G_j \setminus G_{j+1}} \nu_L(a - g(a)) + \sum_{\substack{g \in G_t \\ g \neq e}} \nu_L(a - g(a)).\end{aligned}$$

Using the Corollary to Lemma 5.35 we obtain

$$\nu_L(f'(a)) = \sum_{j=0}^{t-1} (j+1)(\#G_j - \#G_{j+1}) + (t+1)(\#G_t - 1) = \sum_{j=0}^{t} (\#G_j - 1),$$

as asserted. □

Corollary. *If q is a prime, L/K is a normal extension of a $\mathfrak{p}$-adic field K, and $Gal(L/K)$ is a q-group, then*

$$D_{L/K} = I^{q-1}$$

holds with a certain ideal I.

Proof : Since the extension L/K can be obtained by consecutive extensions with Galois group C_q, and $D_{L/K}$ is the product of the differents of those extensions, it suffices to consider the case when $Gal(L/K) \sim C_q$. If L/K is unramified, then the assertion is trivial, as $D_{L/K} = S$, so assume that $e(L/K) > 1$. In this case we get $\#G_0 = q$, and the remaining ramification groups are trivial in the case $q \neq p$, and are isomorphic to C_q if $q = p$, thus in any case $\#G_i - 1 \in \{0, q-1\}$, and the assertion follows from the theorem. □

5.3. Harmonic Analysis in $\mathfrak{p}$-adic Fields

1. In this section we shall apply results from the theory of locally compact Abelian groups to the study of additive and multiplicative groups of a $\mathfrak{p}$-adic field K. The principal facts of that theory may be found in Appendix I.

Observe first that by Theorem 5.6 the groups K^+ and K^* are locally compact, and the same holds for the groups $U_i(K)$, which are moreover compact. Our next aim is the description of the duals of these groups, and later we shall consider the *Mellin transform* in K^*. The principal result of this section is a theorem dealing with the functional equation for the Mellin transform, proved in the thesis of Tate [50].

Throughout this section K will be an extension of degree n of $\mathbb{Q}_p$, R will be its the ring of integers, $\mathfrak{P}$ its prime ideal, π a fixed generator of $\mathfrak{P}$, ν the corresponding exponent, v its valuation, normalized by the requirement

$$v(x) = N(\mathfrak{P})^{-\nu(x)},$$

$U, U_1, \ldots$ will be the unit groups, and $D = D_{K/\mathbb{Q}_p}$.

First we determine the dual group of K^+.

Theorem 5.37. *The group $\hat{K}^+$ is topologically isomorphic to K^+, and every character of K^+ has the form $X(ax)$, where X is a fixed non-trivial character of K^+, and $a \in K^+$. The map $\Phi : a \mapsto X(ax)$ provides the required isomorphism.*

Proof : Fix a non-trivial character X of K^+. Then $X(ax)$ is obviously also a character, and it is clear that the map Φ is an algebraic homomorphism. Let $t \in K^+$ be chosen so that $X(t) \neq 1$. If $a \in \operatorname{Ker} \Phi$, then $X(ax) = 1$ holds for all $x \in K$, whence in the case $a \neq 0$ we get for $x = t/a$ the equality $1 = X(t) \neq 1$, a contradiction. This gives $a = 0$, and so Φ is injective.

Now we prove that Φ is a homeomorphism of K^+ into its dual group. If χ_1 is a character of K^+, then the sets

$$U = U(\epsilon, C) = \{\chi : \ |\chi(x) - \chi_1(x)| < \epsilon \text{ for } x \in C\}$$

(with $\epsilon > 0$ and compact C) form the fundamental system of neighbourhoods of the character χ_1, and so to prove that Φ is continuous it suffices to observe that the set $\Phi^{-1}(U)$ is open, being equal to

$$\{a \in K^+ : \ |\chi_1(x) - X(ax)| < \epsilon \text{ for } x \in C\}.$$

Let V be a fixed non-empty open subset of K. Then

$$\Phi(V) = \{\chi : \ \chi(x) = X(ax) \text{ for } a \in V\}.$$

Let now $X_1(x) = X(ax) \in \Phi(V)$ be fixed. We claim that a suitable neighbourhood of it in the set of characters having the form $X(bx)$ $(b \in K^+)$ with

the topology induced from $\hat{K}^+$ is entirely contained in $\Phi(V)$. Let v be the valuation of K, and choose t with $X(t) \neq 1$. Moreover put

$$\epsilon_0 = |1 - X(t)|, \quad M = 2v(t)/\inf_{x \notin V} v(a-x), \quad C = \{x \in K^+ : \ v(x) \leq M\}.$$

The neighbourhood $U(\epsilon_0, C) \cap \Phi(K^+)$ of X_1 satisfies our requirement. In fact, if $X(bx)$ belongs to it, then for every $x \in C$ we have

$$|X(bx) - X(ax)| < \epsilon_0,$$

i.e.,

$$|1 - X((b-a)x)| < |1 - X(t)|,$$

showing that the element $t/(b-a)$ does not lie in C, thus $v(t/(b-a)) > M$, and we obtain finally

$$v(b-a) < v(t)/M = \frac{1}{2} \inf_{x \notin V} v(a-x),$$

proving $b \in V$. Hence $\Phi(V)$ is open in $\Phi(K^+)$, and we see that

$$\Phi : \ K^+ \longrightarrow \Phi(K^+)$$

is a homeomorphism. The local compactness of K^+ implies the same for $\Phi(K^+)$, and since K is complete, thus $\Phi(K^+)$ is complete, and consequently closed in $\hat{K}^+$. We shall now show that $\Phi(K^+)$ is dense in the dual group of K^+. If it were not dense, then there would exist a non-trivial character χ of that dual group, satisfying $\chi(\psi) = 1$ for $\psi \in \Phi(K^+)$. Since Theorem I of the Appendix I implies the existence of a non-zero $c = c(\chi) \in K^+$ with $\chi(\psi) = \psi(c)$, but every $\psi \in \Phi(K^+)$ is of the form $\psi(x) = X(ax)$, and therefore for all $x \in K^+$ we would have $X(ax) = 1$, implying $xK^+ \neq K^+$, and thus $x = 0$. This shows that the group $\Phi(K^+)$ is dense in K^+, and since it is also closed, the surjectivity of Φ follows. □

In the sequel we shall use a standard choice of the character X. First consider the case $K = \mathbb{Q}_p$, and observe that to every $x \in \mathbb{Q}_p$ one can find a unique rational number $\lambda(x)$ in the interval $[0, 1)$ whose denominator is a power of p, and for which the difference $x - \lambda(x)$ is a p-adic integer. Indeed, every element of $\mathbb{Q}_p$ can be written uniquely in the form

$$x = a_{-N}p^{-N} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots,$$

with $0 \leq a_i < p$, $a_i \in \mathbb{Z}$, and so we may define $\lambda(x) = a_{-N}p^{-N} + \cdots + a_{-1}p^{-1}$ if $x \in \mathbb{Z}_p$, and $\lambda(x) = 0$, if $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$. The function λ is continuous and additive mod 1, i.e. the difference $\lambda(x+y) - \lambda(x) - \lambda(y)$ is a rational integer. Putting

$$X(x) = \exp(2\pi i \lambda(x))$$

we obtain a non-trivial character of $\mathbb{Q}_p^+$. In the general case let $\mathbb{Q}_p \subset K$, and define the standard character by

$$X(x) = \exp(2\pi i \lambda(T_{K/\mathbb{Q}_p}(x))).$$

To see that X is non-trivial write $[K : \mathbb{Q}_p] = p^m q$, with $m \geq 0$ and $p \nmid q$, and consider $x = p^{-m-1}$. Then $T_{K/\mathbb{Q}_p}(x) = q/p$, and obviously the number $\lambda(q/p)$ is not a rational integer.

Now we determine the character group of the additive group of R.

Proposition 5.38. *The dual group of the additive group R^+ is isomorphic to K^+/D^{-1}.*

Proof : The definition of the different shows that we have $T_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p$ if and only if x lies in D^{-1}, and thus the character $X(ax)$ is trivial on R if and only if $a \in D^{-1}$. (We use here the standard fact that every character of a closed subgroup of a locally compact group G can be extended to a character of G). □

2. Theorem 5.16 reduces the study of characters of the multiplicative group K^* to a description of characters of the group U_1, and this will be achieved by applying Theorems IV and V from Appendix I.

Theorem 5.39. *The dual group of U_1 is a discrete p-group. To every character χ of U_1 there corresponds a positive rational integer m such that χ trivializes on U_m. Therefore χ may be regarded as a character of U_1/U_m.*

Proof : By Theorem V of Appendix I the group U_1 can be represented as the inverse limits of the system $\{U_1/U_i\}$ with obvious maps. Hence $\hat{U}_1$ is the direct limit of the groups $\widehat{U_1/U_i}$, which are finite p-groups. Since the maps of the considered system are in fact embeddings, the theorem follows. □

If χ is a non-trivial character of U_1, and $m = m(\chi)$ is the smallest natural number for which the character χ of U_1 trivializes on U_m, then the ideal $\mathfrak{f}_\chi = \mathfrak{P}^m$ is called the *conductor* of χ. For the trivial character χ_0 of U_1 one puts $f_{\chi_0} = R$.

Now let ψ be a character of K^*. Theorem 5.39, Proposition 5.16 and its Corollary 1 imply that every such character is determined by a character χ of U_1, a rational integer $n \in [0, p^f - 2]$ (with $f = f(K/\mathbb{Q}_p)$), and a complex number z on the unit circle, so that for $x = \epsilon \zeta^r \pi^m \in K^*$ (with ζ being a primitive $(p^f - 1)$-th root of unity, $\epsilon \in U_1(K)$, $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ and $m \in \mathbb{Z}$) we have

$$\psi(x) = \chi(\epsilon)\zeta^{nr} z^m.$$

The *conductor* of ψ is by definition the conductor of χ, In the same way we may speak about conductors of characters of any subgroup of K^* containing U_1.

Now we turn to quasicharacters.

Theorem 5.40. *(i) Every quasicharacter of K^+ is a character.*

(ii) Every quasicharacter q of K^* is determined by a pair $[\chi, z]$, where χ is a character of U, and z is a non-zero complex number. If $x = \epsilon\pi^n$ is the canonical form of an element of K^*, then $q(x) = \chi(\epsilon)z^n$,

Proof : (i) It suffices to show that every quasicharacter of K^+ is bounded. To do this observe that the restriction of q to R must be a character, since R is compact. Hence for $x \in R$ we have $|q(x)| = 1$. But every element of K^* can be put in the form x/m with $x \in R$ and a natural m, and since $|q(x/m)|^m = |q(x)| = 1$ we get $|q(x/m)| = 1$.

(ii) Since $U(K)$ is compact, every quasicharacter on it must be a character and we may use the preceding observation. □

It follows from the last theorem that every quasicharacter of K^* is trivial on a certain group U_m. If it is trivial on U, then we call it *unramified*, and if it trivializes on U_m, and m is minimal, then m is called its *ramification degree*, and the ideal $\mathfrak{P}^m$ its *conductor*. For convenience we call $\mathfrak{P}^0 = R$ the conductor of any unramified quasicharacter. We shall write $\mathrm{cond}(q)$ for the conductor of q.

3. In this subsection we shall fix a Haar measure in K^+ to make the inversion formula for the Fourier transform look as simple as possible. We shall also determine a Haar measure in K^*.

First a triviality: we extend the absolute norm of ideals as defined in Chap. 1 to all fractional ideals by multiplicativity, and observe that the following analogue of Proposition 4.7 (i) holds also in $\mathfrak{p}$-adic fields:

Proposition 5.41. *If $\mathbb{Q}_p \subset K$, then the absolute norm of a fractional ideal I of K generates in $\mathbb{Z}_p$ the ideal $N_{K/\mathbb{Q}_p}(I)$,*

Proof : Repeat the proof of Proposition 4.7 (i), replacing in it $\mathbb{Z}$ by $\mathbb{Z}_p$. □

Now we choose the Haar measure μ in K^+ so that the ring R acquires the measure $N(D)^{-1/2}$. Integrals with respect to that measure will be written simply as $\int f(x)d\mu(x)$. The reasons for such a choice become obvious when we prove the following proposition.

Proposition 5.42. *If f is a continuous function in $L_1(K^+)$ whose Fourier transform*

$$\hat{f}(y) = \int_{K^+} f(x)X^{-1}(xy)d\mu(x),$$

(where X is the standard character of K^+) belongs to $L_1(K^+)$, then the following inversion formula holds:

$$f(x) = \int_{K^+} \hat{f}(y)X(xy)d\mu(y) = \hat{\hat{f}}(-x).$$

Proof : We begin with a useful lemma:

Lemma 5.43. *If a is a non-zero element of K, then the measure $\mu(aR)$ of the fractional ideal generated by it equals $N(aR)^{-1}N(D)^{-1/2}$.*

Proof : Choose a power q of the prime p, satisfying $b = qa \in R$. The additive group of bR is of index $N(qR) = q^n$ in aR, and since all cosets have the same measure we get $\mu(aR) = q^n\mu(bR)$. Moreover, the index $[R^+ : (bR)^+]$ is equal to $N(bR)$, thus $\mu(bR) = \mu(R)/N(bR) = N(D)^{-1/2}N(bR)^{-1}$ and finally

$$\mu(aR) = q^n N(D)^{-1/2}N(bR)^{-1} = N(D)^{-1/2}N(aR)^{-1}. \qquad \square$$

Corollary 1. *If I is a fractional ideal of K, then $\mu(I) = N(I)^{-1}N(D)^{-1/2}$.* $\square$

Corollary 2. *If $I = aR$ is a principal fractional ideal of K, then*

$$\mu(I) = v(a)N(D)^{-1/2}.$$

Proof : Observe that our normalization of the valuation implies the equality $v(a) = N(aR)^{-1}$. $\square$

Returning to the proof of the proposition observe that it suffices to check it for one arbitrarily chosen function f. We shall choose the characteristic function of R, which is continuous, since R is both closed and open, and lies in $L_1(K^+)$, because $\mu(R)$ is finite. Its Fourier transform equals

$$\hat{f}(y) = \int_R X^{-1}(xy)d\mu(y),$$

and since the integrand is a character, and we integrate over a compact subgroup, the integral vanishes, except when for all $x \in R$ one has $X(xy) = 1$, in which case $\hat{f}(y) = \mu(R)$. But we already know that $X(xy)$ is trivial for $x \in R$ if and only if $y \in D^{-1}$, and so we arrive at

$$\hat{f}(y) = \begin{cases} N(D)^{-1/2} & \text{if } y \in D^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

The function $\hat{f}$ belongs to $L_1(K^+)$ since D^{-1} is compact. Now we look at the inverse transform

$$\int_{K^+} \hat{f}(y)X(xy)d\mu(y) = N(D)^{-1/2} \int_{D^{-1}} X(xy)d\mu(y).$$

Again the integrand is a character, and we integrate over a compact subgroup. The previous argument is hence applicable, and leads to the conclusion that $X(xy)$ is trivial on D^{-1} if and only if $x \in R$. Taking into account the equality $\mu(D^{-1}) = N(D)^{1/2}$, resulting from Corollary 1 to Lemma 5.43, we obtain

$$N(D)^{-1/2} \int_{D^{-1}} X(xy)d\mu(y) = f(x),$$

as asserted. □

Now it is easy to obtain a Haar integral in the multiplicative group of K:

Proposition 5.44. *If $I(f) = \int_{K^+} f(x)d\mu(x)$ is a Haar integral in K^+, then the functional*

$$C(f) = \int_{K^*} \frac{f(x)}{v(x)} d\mu(x)$$

is a Haar integral in K^*.

Proof : We have to check that if $g(x) = f(ax)$ with $a \in K^*$, then $C(f) = C(g)$, but this follows from the equalities

$$C(g) = \int_{K^*} \frac{f(ax)}{v(ax)} v(a)d\mu(x) = \int_{K^*} \frac{f(ax)}{v(ax)} d\mu(ax) = \int_{K^*} \frac{f(x)}{v(x)} d\mu(x),$$

the crucial point here lying in the identity $d\mu(ax) = v(a)d\mu(x)$, i.e., $\mu(aE) = v(a)\mu(E)$ for measurable $E \subset K$, a fact, which follows from Lemma 5.43. □

In the sequel we shall utilize a multiple μ^* of the Haar measure (with differential $d\mu^*(x)$) in K^* induced from the Haar integral $C(f)$, namely

$$d\mu^*(x) = \frac{N(\mathfrak{P})}{N(\mathfrak{P}) - 1} \frac{dx}{v(x)}.$$

One verifies immediately that this measure gives

$$\begin{aligned} \mu^*(U) &= N(D)^{-1/2}, \\ \mu^*(U_m) &= (N(\mathfrak{P}) - 1)^{-1} N(D)^{-1/2} N(\mathfrak{P})^{-m+1}. \end{aligned} \tag{5.7}$$

In fact,

$$\int_{1+\mathfrak{P}^m} d\mu^* x = \frac{N(\mathfrak{P})}{N(\mathfrak{P})-1} \int_{1+\mathfrak{P}^m} d\mu(x) = \frac{N(\mathfrak{P})}{N(\mathfrak{P})-1} \int_{\mathfrak{P}^m} d\mu(x),$$
$$= (N(\mathfrak{P})-1)^{-1} N(D)^{-1/2} N(\mathfrak{P})^{-m+1}$$

by Corollary 1 to Lemma 5.43, and the invariance of $d\mu(x)$ under shifts.

4. Now we shall consider the Mellin transform in K^* and prove the functional equation for it. The results of this subsection will be used in Chap. 7 to deduce the functional equations for certain classical functions, associated with algebraic number fields.

First we put the quasicharacters q in a convenient form, related to our specific choice of the valuation v. By Theorem 5.40 (ii) we have for $x = \epsilon\pi^m$ (with $\epsilon \in U$) the equality $q(x) = \chi(\epsilon)z^m$ with $\chi \in \hat{U}$, and a non-zero complex z. Now $v(x) = N(\mathfrak{P})^{-m}$, hence $m = -\log v(x)/\log N(\mathfrak{P})$, and $z^m = v(x)^s$ with $s = \log z/\log N(\mathfrak{P})$, where the complex number s is determined only up to a rational integral multiple of $2\pi i/\log N(\mathfrak{P})$. We obtain thus

$$q(x) = \chi(\epsilon)v(x)^s,$$

and we can always assume that $0 \leq \operatorname{Im} s < 2\pi/\log N(\mathfrak{P})$. The real part of s is uniquely determined by q. We shall call it the *exponent* of the quasicharacter q and denote it by $e(q)$. Observe that the equality $e(q) = 0$ is both necessary and sufficient for q to be a character.

We shall call two quasicharacters

$$q(x) = \chi(\epsilon)v(x)^s \quad \text{and} \quad q_1(x) = \chi_1(\epsilon)v(x)^{s_1}$$

equivalent if $\chi = \chi_1$. If the character χ is fixed, then all quasicharacters equivalent to χ are in a one-to-one correspondence with points of the Riemann surface obtained by identifying points on the complex plane whose difference is a rational integral multiple of $2\pi i/\log N(\mathfrak{P})$. This correspondence induces an analytical structure in any fixed equivalence class of quasicharacters. In particular we can consider analytical functions defined on an equivalence class: if $F(q)$ is a complex-valued function defined for quasicharacters q in an equivalence class, then $F(q)$ may be treated as a function of s alone, and we shall say that F is analytic at a point $q(x) = \chi(\epsilon)v(x)^s$, provided it is analytic at s.

Let f be a continuous complex-valued function on K, lying in $L_1(K^+)$, and assume that for every positive t the function $f(x)v(x)^t$ is in $L_1(K^*)$. If $q(x) = \chi(\epsilon)v(x)^s$ is a quasicharacter of K^* with $e(q) > 0$, then the product fq lies in $L_1(K^*)$, and so the formula

$$Z(f,q) = Z(f,\chi,s) = \int_{K^*} f(x)q(x)d\mu^*(x) \tag{5.8}$$

defines, for fixed f and χ, a function of the complex variable s in the half-plane $\operatorname{Re} s > 0$. This function will be called the *zeta-function* associated with f and the equivalence class of quasicharacters determined by χ.

Now we present some examples of zeta-functions. Let $q(x) = \chi(\epsilon)v(x)^s$ and $\mathfrak{P}^N = \mathrm{cond}(q)$.

Proposition 5.45. *(i) The zeta-function of the characteristic function* 1_{U_m} *of* U_m $(m = 1, 2, \ldots,)$ *equals*

$$Z(1_{U_m}, \chi, s) = \begin{cases} (N(\mathfrak{P}) - 1)^{-1} N(D)^{-1/2} N(\mathfrak{P})^{1-m} & \text{if } m \geq N, \\ 0, & \text{if } 1 \leq m \leq N-1, \end{cases}$$

(ii) The zeta-function of the characteristic function 1_U *of* U *equals*

$$Z(1_U, \chi, s) = \begin{cases} N(D)^{-1/2} & \text{if } \chi = 1, \\ 0 & \text{if } \chi \neq 1. \end{cases}$$

(iii) The zeta-function of the function

$$f(x) = \begin{cases} X(x) & \text{if } x \in \mathfrak{P}^{-N} D^{-1}, \\ 0 & \text{otherwise,} \end{cases}$$

where X *is the standard additive character of* K*, equals*

$$Z(f, \chi, s) = \begin{cases} N(D)^{s-1/2}(1 - N(\mathfrak{P})^{-s})^{-1} & \text{if } \chi = 1, \\ \tau_0(\chi) N(D)^{s-1/2} N(\mathfrak{P})^{N(s-1)+1} (N(\mathfrak{P}) - 1)^{-1} & \text{if } \chi \neq 1, \end{cases}$$

where

$$\tau_0(\chi) = \sum_{i=1}^{r} \chi(\epsilon_i) X(\pi^{-m-N} \epsilon_i), \tag{5.9}$$

with $\epsilon_1, \ldots, \epsilon_r$ *being a set of representatives of the cosets* mod U_N *in* U*, and* $\mathfrak{P}^m = D$.

Proof : (i) For $x \in U_m$ we have $x = \epsilon$ and $q(x) = \chi(\epsilon)$, thus

$$Z(1_{U_m}, \chi, s) = \int_{U_m} \chi(\epsilon) d\mu^*(\epsilon) = \begin{cases} \int_{U_m} d\mu^*(\epsilon) & \text{if } m \geq N, \\ 0 & \text{otherwise,} \end{cases}$$

and it remains to use (5.7).

Note that in this case the zeta-function is constant on each equivalence class of quasicharacters, and therefore, although it is originally defined only in the half-plane Re $s > 0$, it can be extended to an entire function.

(ii) In this case one proceeds in a similar way, and again the zeta-function does not depend on s.

(iii) If we write $x = \epsilon_x \pi^{\nu(x)}$ and $D = \mathfrak{P}^m$, then

$$Z(f,\chi,s) = \int_{(D\mathfrak{P}^N)^{-1}} X(x)\chi(\epsilon_x)v(x)^s d\mu^*(x)$$
$$= \sum_{j=-m-N}^{\infty} N(\mathfrak{P})^{-js} \int_{\pi^j U} X(x)\chi(\epsilon_x) d\mu^*(x)$$
$$= \sum_{j=-m-N}^{\infty} N(\mathfrak{P})^{-js} \int_U X(\pi^j x)\chi(x) d\mu^*(x).$$

For $j \geq -m$ we have $\pi^j U \subset D^{-1}$, hence in this case

$$I_j := \int_U X(\pi^j x)\chi(x) d\mu^*(x) = \int_U \chi(x) d\mu^*(x)$$
$$= \begin{cases} 0 & \text{if } N > 0, \text{ i.e. } \chi \neq 1, \\ N(D)^{-1/2} & \text{if } N = 0, \text{ i.e., } \chi = 1, \end{cases}$$

and thus

$$Z(f,\chi,s) = \sum_{j=-m-N}^{-m-1} N(\mathfrak{P})^{-js} I_j + C(\chi) N(D)^{s-1/2} N(\mathfrak{P})^{sN} (1 - N(\mathfrak{P})^{-s})^{-1},$$

where $C(\chi)$ equals 1 if the character χ is trivial, and equals zero otherwise.

We can now dispose of the case $\chi = 1$. In fact, in this case we have $N = 0$, thus the sum occurring in the above expression is void, and $C(\chi) = 1$, hence we obtain our assertion.

If χ is non-trivial, then we have to compute the integrals I_j for $-m-N \leq j \leq -m-1$. It will turn out that they all vanish, except for I_{-m-N}.

Observe first that the value of the character $X(t)$ depends only on the coset mod D^{-1} determined by t. Note, moreover that the set $\pi^j U$ consists of full cosets mod D^{-1}, because if $a \in \pi^j U$, i.e., $\nu(a) = j$, and the difference $b - a$ lies in D^{-1}, then in view of $j < -m$ we get $\nu(b) = j$.

Now let $j \neq -m-N$. With suitable $a_1, \ldots, a_k \in \pi^j U$ lying in different cosets mod D^{-1} we have

$$\pi^j U = \bigcup_{i=1}^{k} (a_i + D^{-1}),$$

and therefore

$$I_j = \sum_{i=1}^{k} X(a_i) \int_{A_i} \chi(x) d\mu^*(x),$$

where $A_i = (a_i + D^{-1})\pi^{-j} = a_i \pi^{-j}(1 + \mathfrak{P}^{-m-j})$. But

$$\int_{A_i} \chi(x) d\mu^*(x) = \chi(a_i \pi^{-j}) \int_{1+\mathfrak{P}^{-m-j}} \chi(x) d\mu^*(x),$$

and since χ is non-trivial on $1+\mathfrak{P}^{-m-j}$, the last integral vanishes. We see thus that our zeta-function equals

$$N(\mathfrak{P})^{(m+N)s} I_{-m-N},$$

and so it remains to reduce the integral I_{-m-N} to a handy form. Since the character χ is constant on the cosets mod U_N in U, we obtain

$$I_{-m-N} = \sum_{i=1}^{r} \chi(\epsilon_i) \int_{\epsilon_i U_N} X(\pi^{-m-N}x) d\mu^*(x),$$

but since $x \in \epsilon_i U_N$ implies

$$\pi^{-m-N}x \in \pi^{-m-N}\epsilon_i + D^{-1},$$

thus $X(\pi^{-m-N}x) = X(\pi^{-m-N}\epsilon_i)$, and we obtain

$$\begin{aligned} I_{-m-N} &= \sum_{i=1}^{r} \chi(\epsilon_i) X(\pi^{-m-N}\epsilon_i) \int_{\epsilon_i U_N} d\mu^*(x) = \tau_0(\chi) \int_{U_N} d\mu^*(x) \\ &= \tau_0(\chi)(N(\mathfrak{P})-1)^{-1} N(D)^{-1/2} N(\mathfrak{P})^{-N+1}. \end{aligned}$$

Using (5.9) we arrive at our assertion. □

5. Now we can prove the promised functional equation for zeta-functions:

Theorem 5.46. *Let f be a continuous complex-valued function on K, which belongs to $L_1(K^+)$. Assume moreover that its Fourier transform*

$$\hat{f}(y) = \int_{K^+} f(x) X^{-1}(xy) dx$$

also belongs to $L_1(K^*)$. Finally assume that for all $t > 0$ the functions $f(x)v(x)^t$ and $\hat{f}(x)v(x)^t$ lie in $L_1(K^+)$. If we denote by $\hat{q}$ the quasicharacter of K^* defined by $\hat{q}(x) = q^{-1}(x)v(x)$, then for all quasicharacters q with $0 < e(q) < 1$ the corresponding zeta-function satisfies the following functional equation:

$$Z(f,q) = \rho(q) Z(\hat{f}, \hat{q}), \tag{5.10}$$

where

$$\rho(q) = \begin{cases} N(D)^{s-1/2}(1-N(\mathfrak{P})^{s-1})(1-N(\mathfrak{P})^{-s})^{-1} & \text{if } N=0, \\ \tau_0(\chi) N(D)^{s-1/2} N(\mathfrak{P})^{N(s-1)} & \text{if } N \neq 0, \end{cases}$$

where N is defined by $\mathrm{cond}(q) = \mathfrak{P}^N$, and τ_0 is defined by (5.9).

Proof: Let f, g be functions on K, both satisfying the conditions imposed on f in our theorem, and observe that in view of $e(\hat{q}) = 1 - e(q)$ the condition $0 < e(q) < 1$ ensures the existence of all integrals occurring below.

We have

$$Z(f,q)Z(\hat{g},\hat{q}) = \iint_{K^*\times K^*} f(x)\hat{g}(y)q(xy^{-1})v(y)d\mu^*(x)d\mu^*(y),$$

and making the substitution $t = yx^{-1}$ we obtain

$$Z(f,q)Z(\hat{g},\hat{q}) = \int_{K^*}\left(\int_{K^*} f(x)\hat{g}(tx)v(x)d\mu^*(x)\right) q(t^{-1})v(t)d\mu^*(t).$$

We show now that the inner integral is symmetrical in f and g, and this will produce the equality

$$Z(f,q)Z(\hat{g},\hat{q}) = Z(g,q)Z(\hat{f},\hat{q}). \tag{5.11}$$

In fact, noting that $v(x)d\mu(u)\cdot d\mu^*(x) = v(u)d\mu(x)\cdot d\mu^*(u)$, and the sets K^* and K^+ differ only in one element, we obtain

$$\begin{aligned}\int_{K^*} f(x)\hat{g}(tx)v(x)d\mu^*(x) &= \int_{K^*} f(x)v(x)\int_{K^+} g(u)\overline{X(xtu)}d\mu(u)d\mu^*(x)\\ &= \iint_{K^+\times K^*} f(x)g(u)v(x)\overline{X(xtu)}d\mu(u)d\mu^*(x)\\ &= \int_{K^*} g(u)v(u)\int_{K^+} f(x)\overline{X(xtu)}d\mu(x)d\mu^*(u) =\\ &= \int_{K^*} g(u)\hat{f}(ut)v(u)d\mu^*(u).\end{aligned}$$

Now let us fix an equivalence class $\{q:\ q(x) = \chi(\epsilon_x)v(x)^s\}$, determined by a character χ of U, and let $\mathrm{cond}(\chi) = \mathfrak{P}^N$. We specify now the function g, by putting

$$g(x) = \begin{cases} X(x) & \text{if } x\in D^{-1}\mathfrak{P}^{-N},\\ 0 & \text{otherwise.}\end{cases}$$

This gives

$$\begin{aligned}\hat{g}(y) &= \int_{D^{-1}\mathfrak{P}^{-N}} X(x)X(-xy)d\mu(x) = \int_{D^{-1}\mathfrak{P}^{-N}} X(x(1-y))d\mu(x)\\ &= \begin{cases} N(D)^{1/2}N(\mathfrak{P})^N & \text{if } N\neq 0, y\in U_N,\\ N(D)^{1/2} & \text{if } N=0, y\in R,\\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

The zeta-functions for g and $\hat{g}$ were computed in Proposition 5.45, with the exception of $Z(\hat{g},q)$ in the case $N=0$. But in this case we have $q(x) = v(x)^s$, thus

$$\begin{aligned}Z(\hat{g},q) &= \int_{R\setminus\{0\}} N(D)^{1/2}v(x)^s d\mu^*(x) = \sum_{j=0}^{\infty}\int_{\pi^j U} N(D)^{1/2}v(x)^s d\mu^*(x)\\ &= \sum_{j=0}^{\infty} N(\mathfrak{P})^{-js}N(D)^{1/2}\int_{\pi^j U} d\mu^*(x) = (1-N(\mathfrak{P})^{-s})^{-1}.\end{aligned}$$

Finally we arrive at

$$Z(\hat{g},\hat{q}) = \begin{cases} N(\mathfrak{P})/(N(\mathfrak{P})-1) & \text{if } N \neq 0, \\ (1-N(\mathfrak{P})^{s-1})^{-1} & \text{if } N = 0, \end{cases}$$

and we see that the quotient $Z(g,q)/Z(\hat{g},\hat{q})$ equals $\rho(q)$. This, in view of the equality (5.11), implies the theorem. □

Corollary. *Under the assumptions of the theorem the zeta-function $Z(f,q)$ is for every fixed equivalence class of quasicharacters a regular function of s in the half-plane* Re $s > 0$, *and can be prolonged analytically to a meromorphic function.*

Proof : We begin with the regularity. Let $\sigma = \text{Re } s > 0$, $|h| \leq 1$, and consider the difference

$$\frac{Z(f,\chi,s+h) - Z(f,\chi,s)}{h} - \int_{K^*} f(x)\chi(\epsilon_x)v(x)^s \log v(x) d\mu^*(x)$$
$$= \int_{K^*} f(x)\chi(\epsilon_x)v(x)^s \left(\frac{v(x)^h - 1}{h} - \log v(x) \right) d\mu^*(x).$$

We shall prove that this difference tends to 0 with h. We can write it in the form

$$h \int_{K^*} f(x)\chi(\epsilon_x)v(x)^s \sum_{j=2}^{\infty} h^{j-2} \frac{\log^j v(x)}{j!} d\mu^*(x),$$

and so it does not exceed

$$|h| \int_{K^*} |f(x)|v(x)^\sigma \sum_{j=2}^{\infty} |h|^{j-2} \frac{|\log^j v(x)|}{j!} d\mu^*(x).$$

We split the last expression in two parts: the first, I_1, extended over the set $\{x : v(x) \geq 1\}$, and the second, I_2, extended over the remaining part of K^*.

Since

$$I_1 \leq |h| \int_{v(x)\geq 1} |f(x)|v(x)^{1+\sigma} d\mu^*(x),$$

we see that $\lim_{h\to 0} I_1 = 0$. To evaluate I_2 choose a constant $B \geq 4/\sigma^2$, and let $|h| \leq (\sigma/2)^3$. Then for $j = 2,3,\ldots$ we have $|h|^{j-2} \leq B(\sigma/2)^j$, and thus I_2 does not exceed

$$|h| \int_{v(x)<1} |f(x)|v(x)^\sigma B \exp(-\frac{\sigma}{2} \log v(x)) d\mu^*(x)$$
$$= B|h| \int_{v(x)<1} |f(x)|v(x)^{\sigma/2} d\mu^*(x),$$

and therefore $\lim_{h\to 0} I_2 = 0$.

Now observe that since $\rho(q) = \rho(\chi, s)$ with a fixed χ is a meromorphic function of s, the functional equation (5.10) can be used for the prolongation of $Z(f, q)$ to a meromorphic function of s, since for $\operatorname{Re} s < 1$ the right-hand side of (5.10) is well-defined and regular up to the poles of $\rho(q)$. In view of the theorem the two definitions of $Z(f, q)$ in the strip $0 < \operatorname{Re} s < 1$ (one direct and the other via the functional equation) agree with each other. □

It should be pointed out that the zeta-functions can have their poles only at the poles of $\rho(q)$. Moreover, the last theorem shows the importance of the sum $\tau_0(\chi)$ for the general theory, and not only as a factor of the zeta-function of a particular function. In the next chapter we shall say more about this sum, and now let us return to the factor $\rho(q)$, occurring in (5.10).

Proposition 5.47. *If for a quasicharacter q we denote by $\hat{q}$ the quasicharacter $q^{-1} \cdot v$, then we have:*
(i) $\rho(\hat{q}) = q(-1)\rho(q)^{-1}$,
(ii) $\rho(\overline{q}) = q(-1)\overline{\rho(q)}$,
(iii) If $e(q) = 1/2$ *and* $\mathrm{cond}(\chi) = \mathfrak{P}^N$ *with* $N \neq 0$, *then* $|\rho(q)| = 1$, *whence* $|\tau_0(\chi)| = N(\mathfrak{P}^N)^{1/2}$.

Proof: (i) Let f be a function , satisfying the assumptions of Theorem 5.46, and whose zeta-function $Z(f, q)$ does not vanish at q. Such functions exist, e.g. one can take for f the function occurring in part (iii) of Proposition 5.45. The functional equation implies

$$Z(f, q) = \rho(q) Z(\hat{f}, \hat{q}) = \rho(q)\rho(\hat{q}) Z(\hat{\hat{f}}, \hat{q}).$$

But $\hat{\hat{f}}(x) = f(-x)$ and $\hat{\hat{q}}(x) = q(x)$, whence

$$Z(\hat{\hat{f}}, \hat{\hat{q}}) = \int_{K^*} f(-x) q(x) d\mu^*(x) = q(-1) \int_{K^*} f(x) q(x) d\mu^*(x),$$

thus $Z(\hat{\hat{f}}, \hat{\hat{q}}) = q(-1) Z(f, q)$, and $Z(f, q) = \rho(q)\rho(\hat{q}) q(-1) Z(f, q)$, leading to

$$q(-1)\rho(q)\rho(\hat{q}) = 1,$$

i.e., in view of $q(-1) = \pm 1$, $\rho(q)\rho(\hat{q}) = q(-1)$.

(ii) This time let f be a function satisfying the assumptions of Theorem 5.46, such that the zeta-function of its Fourier transform does not vanish at $\hat{q}$ (here again the function from Proposition 5.45 will do). Then

$$\overline{Z(f, q)} = Z(\overline{f}, \overline{q}) = \rho(\overline{q}) Z(\hat{\overline{f}}, \hat{\overline{q}}),$$

and in view of $\overline{\hat{q}} = \hat{\overline{q}}$ and

$$\hat{\overline{f}}(x) = \int_K \overline{f}(y)\overline{X(xy)}d\mu(y) = \overline{\int_K f(y)X(xy)d\mu(y)} = \overline{\hat{f}(-x)}$$

we obtain

$$Z(\hat{\overline{f}},\hat{\overline{q}}) = \int_{K^*} \hat{\overline{f}}(x)\hat{\overline{q}}(x)d\mu^*(x) = \overline{\int_{K^*} \hat{f}(-x)\hat{q}(x)d\mu^*(x)}$$
$$= \hat{q}(-1)\overline{\int_{K^*} \hat{f}(x)\hat{q}(x)d\mu^*(x)} = q(-1)\overline{Z(\hat{f},\hat{q})}.$$

Now the functional equation implies

$$\overline{Z(f,q)} = \overline{\rho(q)}\overline{Z(\hat{f},\hat{q})},$$

and using the equality $\overline{Z(f,q)} = \rho(\overline{q})q(-1)\overline{Z(\hat{f},\hat{q})}$ we arrive at $q(-1)\rho(\overline{q}) = \overline{\rho}(q)$, which implies (ii).

(iii) If $e(q) = 1/2$, then $|q(x)| = \sqrt{v(x)}$, thus

$$q(x)\overline{q}(x) = v(x) = q(x)\hat{q}(x),$$

i.e., $\overline{q}(x) = \hat{q}(x)$. Applying (i) and (ii) we obtain

$$q(-1)\rho(q)^{-1} = \rho(\overline{q}) = q(-1)\overline{\rho}(q)$$

and $\rho(q)^{-1} = \overline{\rho}(q)$, showing the truth of (iii). □

5.4. Notes to Chapter 5

1. The p-adic and $\mathfrak{p}$-adic fields were introduced by Hensel in a remarkable sequence of papers (Hensel [97c], [02], [04], [05a], [09]), and culminating in two books (Hensel [08], [13]). He defined p-adic numbers as formal Laurent series in p with suitably defined arithmetic operations. The approach based on valuations is due to Kürschak [13], and an axiomatical approach was made by Fraenkel [12].

With regard to Theorem 5.4 let us remark that if K is a field with a topology induced by a non-Archimedean valuation, then it will be locally compact if and only if it is complete, the valuation is discrete, and the residue class-field is finite. The theorem of Hasse and F.K.Schmidt [33] implies that every such field either is $\mathfrak{p}$-adic, or is a finite extension of the field of formal power series over a finite field. The original proof was incomplete, as pointed out by Mac Lane [39a] (cf. Chao [51]). Other proofs were given in Mac Lane [39b], Teichmüller [36], [37], Witt [36]. Our Theorem 5.10 is a part of this result.

Fields with a topology induced by a valuation were described by Shafarevich [43] (cf. Dürbaum, Kowalsky [53], Fleischer [53], Kaplansky [47], Zelinsky [48]). Surveys of the theory of topological fields were given in Shell [90], Warner [89], and Więsław [85].

2. Hensel's lemma (Theorem 5.6) was proved in Hensel [04] for the field $\mathbb{Q}_p$, and in Hensel [05a] for $K_\mathfrak{p}$ in a form equivalent to that given by us, which appeared first in Hensel [18]. (It has been pointed out in Ore [27] that a form of Hensel's lemma occurs already in a paper of Schönemann [46,sect.59].) For other forms of Hensel's lemma see Hensel [08], [13], Rella [24b]. For certain interesting applications see Dalen [55], Liang, Mead [83],

Fields with a non-Archimedean valuation in which the analogue of Hensel's lemma holds are called *relatively complete*. They were studied by Ostrowski [35], who showed that a field is relatively complete if and only if it is closed under separable algebraic extensions in its completion. Examples of relatively complete fields which are not complete were given earlier in Ostrowski [13]. It was shown in Rim [57] that a field K is relatively complete if and only if its valuation has a unique extension to the algebraic closure of K. Cf. Inaba [52], Nagata [53], Neukirch [68], Rayner [57], [58], Schilling [43], Zassenhaus [54].

3. The corollaries 1-4 to Theorem 5.6 are due to Hensel For further applications of Hensel's lemma see Hensel [08], Thurston [43]. Corollary 3 implies that the field $\mathbb{Q}_p$ contains subfields, which are normal extensions of the rationals with Galois group equal to C_2^m for $m = 1, 2, \ldots$, and Kleiman [71] proved that the same holds for normal extensions $K/\mathbb{Q}$ having symmetric Galois group S_n with $n \leq p$. Cf. Frey, Geyer [72], Iwata [72]. Cassels [76] deduced from Hensel's lemma that every finitely generated extension of the rationals is embeddable in infinitely many fields $\mathbb{Q}_p$. For finite extensions this can be deduced from Theorem 4.37.

4. Proposition 5.8 (Krasner's lemma) was proved in Krasner [46]. Conditions for an isomorphism of two extensions of $\mathbb{Q}_p$ were given in Hensel [09] (cf. Krasner [37a,c]). Proposition 5.13 was proved in Hensel [18].

The definition of the discriminant $\partial(L/K)$, as well as Proposition 5.14 and Theorem 5.15 are due to Fröhlich [60b].

5. For the construction of an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ see Bauer [24]. The p-adic valuation has a unique extension to $\overline{\mathbb{Q}}_p$, however $\overline{\mathbb{Q}}_p$ is not complete (Ostrowski [13], [17]). It has been proved by Kürschak [13] and Rychlik [24] that the completion Ω_p of $\overline{\mathbb{Q}}_p$ is both algebraically closed and complete. There is an extensive theory of functions in Ω_p. See Gouvêa [93], Koblitz [77], Mahler [73], Washington [82], where also further references may be found.

For a $\mathfrak{p}$-adic field K put $G(K) = Gal(\overline{K}/K)$. A study of this group was made by Iwasawa [55b], and a fully satisfactory description of its structure was in the case $\mathbb{Q}_p \subset K$ with odd p given in Janssen [82], Janssen, Wingberg [82]. For the case $p = 2$, $\zeta_4 \in K$ see Diekert [84], Zelvenskiĭ [72], [78], [82]. Note that $G(K)$ does not determine K, as shown in Yamagata [76] (cf. Jarden, Ritter [79], [80], Jenkner [92], Ritter [78]). Automorphisms of $G(K)$ were studied in Jarden, Ritter [79], [80].

Let $G_p(K)$ be the Galois group of the minimal extension of K closed under p-extensions. If K is regular, then, as shown in Shafarevich [47], $G_p(K)$ is a free topological group with $1+n$ free generators, where $n = [K : \mathbb{Q}_p]$. If K is irregular K, then $G_p(K)$ has $n+2$ topological generators and one relation (Kawada [54]; cf. Faddeev, Skopin [59], Miki [76]). Earlier results on this topic are described in the book of Koch [70].

6. Theorem 5.21 was proved in Hensel [14b]. See also Halter-Koch [72a], Hasse [49], Hasse, Hensel [23], Hensel [15], [16a,b], [17], [21c], [27], Rella [20], Wahlin [16], [32]. In the next chapter we shall describe all situations in which the factor group $U(K)/U_n(K)$ is cyclic. For an interpretation of U_1/U_n in terms of algebraic groups see Kambayashi [75].

The p-adical logarithm occurring in the proof of Proposition 5.22 was introduced in Hensel [15]. For another definition of it, leading easily to its main properties see Leopoldt [61] (cf. Disse [25], [26], Pollaczek [46]).

7. Most of the results of Section 2 are due to Hensel [08], in particular the Theorems 5.26, 5.27 and 5.29. Tame extensions were discussed in Albert [40], where also a new proof of Corollary 3 to Theorem 5.34 is given. Another proof was given in Bauer [22]. Ramified cyclic extensions of degree p of fields containing $\mathbb{Q}_p$ were treated in MacKenzie, Whaples [56], and for non-normal extensions of degree p this was done in S.Amano [71].

Corollary 2 to Theorem 5.27 appears in Hensel [09] (cf. Albert [40]). The number of extensions with prescribed properties of a given $\mathfrak{p}$-adic field was studied in a series of papers by Krasner [37b], [38], [62], [66]. In particular he obtained the following formula for the number $N_K(n)$ of all extensions of degree n of a $\mathfrak{p}$-adic field, containing $\mathbb{Q}_p$:

$$N_K(n) = \sigma(h)\left(\frac{p^{m+1}-1}{p-1} + S\right),$$

where $n = hp^m$ with $p \nmid h$, $\sigma(h)$ is the sum of positive divisors of h, and

$$S = \sum_{j=1}^{\infty} \left(p^{m+j+1} - p^{2j}\right) \frac{p^{\epsilon(j)N} - p^{\epsilon(j-1)N}}{p-1},$$

$\epsilon(s)$ being defined by

$$\epsilon(j) = \begin{cases} \frac{1}{p} + \cdots + \frac{1}{p^j} & \text{if } j \geq 1, \\ 0 & \text{if } j = 0, \end{cases}$$

and $N = n[K : \mathbb{Q}_p]$. He proved also that number of fully ramified extension of degree n of any $\mathfrak{p}$-adic field is divisible by p.

For other results on the number of extensions of $\mathfrak{p}$-adic fields see Bayer, Rio [99], Feit [59], Fujisaki [90], [89], Krasner [79], Massy, Nguyen-Quang-Do [75], Naito[95], Payan [65], Serre [78], Travesa [90b], Yamagishi [95].

A method of finding the defining polynomials of extensions of $\mathbb{Q}_p$ of given degree gave Pauli, Roblot [01].

Ramification groups were defined by Hilbert [94a] for finite extensions of algebraic number fields. In the p-adic case they were apparently first used in Ore [28b]. For characterizations of the sequence of ramification groups see Maus [68], [73], Miki [77], Sueyoshi [84]. See Serre [62] and the literature quoted there for more information on ramification groups.

8. Let L/K be a normal extension of $\mathfrak{p}$-adic fields with Galois group G, and let R, S be the corresponding rings of integers. It was observed by Noether [32] that L/K is tame if and only if S and $R[G]$ are isomorphic as $R[G]$-modules (for an elementary proof see Kawamoto [86]). Hence the problem of the existence of a normal basis is solved completely for such extensions.

Leopoldt [59] showed that if $K/\mathbb{Q}_p$ is Abelian with Galois group G, then the ring R of integers of K is a free module over the associated order

$$A_K = \{\sigma \in Z_p[G] : \ \sigma(R) \subset R\}$$

(cf. Letttl [90a]). This may be not true for non-Abelian, even unramified, extensions of $\mathbb{Q}_p$, as shown by Bergé [78]. Leopoldt's result has been extended in Lettl [98], who showed that under the same assumptions, R is free over A_L for every extension of Q_p, contained in K.

For further results concerning the Galois structure of $\mathfrak{p}$-adic rings see Bertrandias [78], [79], Bertrandias, Bertrandias, Ferton [72], [73], Borevich, Vostokov [73], Burns [91], Chan, Lim [95], Elder [95], Elder, Madan [94], Ferton [72], [73], [74], [75], Martel [74], Y.Miyata [74], [79], [80], [95], Ullom [70], Vostokov [74], [76a,b].

9. If $\mathbb{Q}_p \subset K$ and L/K is normal with Galois group G, then one can consider $U_1(L)$ as an $\mathbb{Z}_p[G]$-module. In fact, if $u \in U_1(L)$ and $A = \sum_{g\in G} a_g g \in Z_p[G]$, then the action of A upon u can be defined by

$$u^A = \prod_{g\in G} g(u)^{a_g},$$

which is well-defined, since G preserves the prime ideal, and so $g(U_1(L)) = U_1(L)$ holds for $g \in G$. If $U_1(L)$ is, as $\mathbb{Z}_p[G]$-module, the direct sum of a finite module and a free module, then the extension L/K is said to have a *normal basis for units*. Krasner [39] proved for regular fields L that if L/K is tame, then such a basis exists, and the converse implication was established by Gilbarg [42]. In the irregular case Krasner [39] and Borevich [65a] demonstrated that tame ramification is neither necessary nor sufficient, and the complete solution of the problem was obtained in Borevich, Skopin [65]. We quote it only in the case when L/K is tame and $p \neq 2$. In this case L/K has a normal basis for units if and only if the index $[L : K(\zeta_{p^s})]$ (where s is the irregularity index of L) is not divisible by p.

The structure of $U_1(L)$ as a $\mathbb{Z}_p[G]$-module was treated for various classes of extensions in Arutyunyan [77], Borevich [64], [65a,b], [67], Borevich , Gerlovin [76], David [78], Gerlovin [69], Iwasawa [60], Krasner [36], Pieper [72], [73], Rosenbaum [66], [70], Wahlin [32], Wingberg [79].

10. The results of Section 3 are due to Tate [50]. For a simple proof of Theorem 5.37 see Washington [74]. More about Gaussian sums defined by (5.9) will be said in the next chapter.

The class-field theory in $\mathfrak{p}$-adic fields establishes a one-to-one correspondence between Abelian extensions L/K of a given $\mathfrak{p}$-adic field K and subgroups $H \subset K^*$ of finite index. This correspondence implies $H = N_{L/K}(L^*)$ and $Gal(L/K) \sim K^*/H$. See the books of G.Gras [03], Hazewinkel [69], Iwasawa [80], [86], Neukirch [86], [92], Serre [62]. See also Fesenko [96], and the exposition of Serre in Cassels, Fröhlich [67]. For a quick introduction see Hazewinkel [75].

Every Abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension (see Lubin [81], Rosen [81]). This is an analogue of the Kronecker-Weber theorem, which will be established in Chap. 6 (see Theorem 6.18).

11. An integral domain R is called a *BC-domain* (domain with bounded cycles) if for every $N \geq 1$ there exists a number $M(N, R)$ with the property that if $\Phi : R^N \longrightarrow R^N$ is a map defined by N polynomials with coefficients from R in N variables, and there exist distinct points $P_1, \ldots, P_k \in R^N$ such that $\Phi(P_i) = P_{i+1}$ $(i = 1, 2, \ldots, k-1)$, and $\Phi(P_k) = P_1$, then $k \leq M(N, R)$. Each such P_j is said to be a *periodic point* of Φ. It has been shown by Pezda [94b] that rings of integers of $\mathfrak{p}$-adic fields are BC-domains. The case $N = 1$ was earlier considered in Pezda [94a]. Periodic points of power series over $R_{\mathfrak{p}}$ were studied in Li [96].

Since every ring R_K can be embedded in a suitable ring Z_p it follows that R_K is also a BC-domain. In case $N = 1$ this was earlier established in Narkiewicz [89]. In this case one can show that finite polynomial orbits have a bounded cardinality (Narkiewicz, Pezda [97]), and it is possible to classify them (Halter-Koch, Narkiewicz [99], [00] (cf. Marszałek, Narkiewicz [04]). In the p-adic case such bounds do not exist.

See also Morton, Patel [94], Morton, Silverman [94], [95], Pezda [03].

EXERCISES

1. Prove that the algebraic closure of $\mathbb{Q}_p$ is not complete.

2. Prove that the completion of the algebraic closure of $\mathbb{Q}_p$ is algebraically closed.

3. Prove that every automorphism of $\mathbb{Q}_p$ is continuous.

4, Prove that for every prime p and $n \geq 3$ one can find a polynomial irreducible over $\mathbb{Z}$ of degree n, which has a root in $\mathbb{Q}_p$, but does not split there in linear factors.

5. Let L/K be a finite extension of a $\mathfrak{p}$-adic field, and let R, S be the corresponding rings of integers. Prove that the set of all $a \in S$ satisfying $S = R[a]$ is open.

6. (a) Let K be a $\mathfrak{p}$-adic field containing $\mathbb{Q}_p$, and let $p \nmid n$. Determine the Galois group of the splitting field of $X^n - 1$ over K.

(b) Show that if n is a power of p and $K = \mathbb{Q}_p(\zeta_n)$, then the Galois group of $K/\mathbb{Q}_p$ is isomorphic to the multiplicative group of residue classes mod n, prime to n.

7. Prove that if L/K is unramified, then for $n = 1, 2, \ldots$ the norm map $N_{L/K}$ maps $U_n(L)$ onto $U_n(K)$.

8. Prove that if $[K : \mathbb{Q}_p] = n$ and $D = D_{K/\mathbb{Q}_p}$, then the groups K^+/D^{-1} and $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ are topologically isomorphic.

9. (Hensel [94a]) Prove that if K is a $\mathfrak{p}$-adic field and $D_{L/K} = \mathfrak{P}^m$, then $m \leq e(L/K) + \nu(e(L/K)) - 1$, where ν denotes the exponent in L.

10. Let $K/\mathbb{Q}$ be a finite extension. Show that for infinitely many primes p there exists an embedding of K in $\mathbb{Q}_p$.

11. Describe all cubic extensions of the fields $\mathbb{Q}_2$ and $\mathbb{Q}_3$.

12. Let R be the ring of integers in a $\mathfrak{p}$-adic field $K \supset \mathbb{Q}_p$, put $A_N = R/\mathfrak{P}^N$, let π be a fixed generator of $\mathfrak{P}$, and $e = e(K/\mathbb{Q}_p)$, $f = f(K/\mathbb{Q}_p)$.

(a) Prove that for $N = 1, 2, \ldots, e$ one has $pA_N = 0$ and $A_N^+ \sim C_p^{fN}$.

(b) Show that if $M > N$, then $\pi^N A_M^+ \sim A_{M-N}^+$.

(c) Let $k \geq 1$ and assume that $(k-1)e < N \leq ke$. Prove that

$$A_N^+ \sim C_{p^{k-1}}^a \oplus C_{p^k}^b,$$

where $a = (ke - N)f$ and $b = (N - ke + e)f$.

6. Applications of the Theory of $\mathfrak{p}$-adic Fields

6.1. Arithmetical Applications

1. In this chapter we shall apply results obtained in Chap. 5 to the study of algebraic number fields. The first section contains direct arithmetic applications, and in the second we introduce the ring of adeles and the group of ideles, study their principal proprieties and perform some harmonic analysis, including the deduction of the functional equation for suitably defined zeta-functions.

In this section K will be an algebraic number field, and L/K an extension of degree n. By $\mathfrak{p}$ we shall denote a non-zero prime ideal in R_K, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ will be the prime ideals of R_L, lying above $\mathfrak{p}$. R will denote the ring of integers of $K_\mathfrak{p}$ and S_i will be the ring of integers of $L_{\mathfrak{P}_i}$. If the prime ideal $\mathfrak{P}_i$ will be fixed, then we shall denote it by $\mathfrak{P}$, and write S instead of S_i.

The method of transferring results from the $\mathfrak{p}$-adic case to number fields is, broadly speaking, the following: we shall consider the $\mathfrak{p}$-adic fields $K_\mathfrak{p}$ and $L_{\mathfrak{P}_i}$ $(i = 1, 2, \ldots, m)$. By Theorem 5.11 the fields $L_{\mathfrak{P}_i}$ are finite extensions of $K_\mathfrak{p}$, and by part (iv) of that theorem the corresponding ramification indices and prime ideal degrees are not affected by this localization. Now, having a problem concerning the extension L/K, we can try to solve the corresponding problem in $L_{\mathfrak{P}_i}/K_\mathfrak{p}$ for all $\mathfrak{p}$, which may be easier, since we have additional topological means at our disposal, and the rings of integers in $\mathfrak{p}$-adic fields are principal ideal domains. Having done this, we can try to put the local solutions together in some way, and, if we are lucky, this may yield a solution to the original problem.

Proposition 6.1. *Let $L = K(a)$ with $a \in R_L$, and denote by F the minimal polynomial of a over R_K. If $\mathfrak{p}$ is a prime ideal of R_K, and in the field $K_\mathfrak{p}$ one has the factorization $F = F_1 \cdots F_m$ into irreducible polynomials, then*

$$\mathfrak{p}R_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_m^{e_m},$$

where $\mathfrak{P}_i$ are distinct prime ideals of R_L and $e_i f_{L/K}(\mathfrak{P}_i) = \deg F_i$ holds for $i = 1, 2, \ldots, m$.

Moreover, for each i one has $L_{\mathfrak{P}_i} \sim K_\mathfrak{p}(b_i)$ with $F(b_i) = 0$, and there is a topological isomorphism between the $K_\mathfrak{p}$-spaces $\bigoplus_i L_{\mathfrak{P}_i}$ and $L \otimes_K K_\mathfrak{p}$.

Proof : For each $i = 1, 2, \ldots, n$ consider the field M_i, generated over $K_\mathfrak{p}$ by one of roots, say b_i, of the polynomial F_i. By Propositions 3.2 and 5.7 the field M_i is complete under the unique extension of the valuation of $K_\mathfrak{p}$ to M_i, and contains an isomorphic copy of L, namely $K(b_i)$. Moreover, M_i coincides with the closure of $K(b_i)$, because that closure contains $K_\mathfrak{p}$ as well as b_i. If ν is the exponent in M_i, induced by its valuation, then its restriction to $K(b_i) \sim L$ corresponds to a prime ideal $\mathfrak{P}_i$, lying above $\mathfrak{p}$, and we obtain that M_i is isomorphic with $L_{\mathfrak{P}_i}$ under a valuation-preserving isomorphism. This, together with Theorem 5.11 (i) proves all but the last assertion of our proposition. To prove the last one note that by the already proved part and Theorem 4.5 we have

$$\dim_{K_\mathfrak{p}} \bigoplus_{i=1}^{n} L_{\mathfrak{P}_i} = [L : K] = \dim_{K_\mathfrak{p}} L \otimes_K K_\mathfrak{p},$$

and it remains to apply Proposition 3.2. □

Corollary. *If $x \in L$, then*

$$N_{L/K}(x) = \prod_{i=1}^{m} N_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x), \quad T_{L/K}(x) = \sum_{i=1}^{m} T_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x).$$

Proof : If x generates the extension L/K, then the asserted equalities follow immediately from the proposition. If, however, $M = K(x)$ is a proper subfield of L, $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ are the prime ideals of R_M lying above $\mathfrak{p}$, and for each $i = 1, 2, \ldots, s$ we denote by $\mathfrak{P}_{1i}, \ldots, \mathfrak{P}_{k_i i}$ the prime ideals of R_L lying over $\mathfrak{Q}_i$, then

$$N_{L/K}(x) = N_{M/K}(N_{L/M}(x)) = (N_{M/K}(x))^{[L:M]} = \prod_{i=1}^{s} (N_{M_{\mathfrak{Q}_i}/K_\mathfrak{p}}(x))^{[L:M]},$$

but, on the other hand, we have

$$N_{L_{\mathfrak{P}_{ji}}/M_{\mathfrak{Q}_i}}(x) = x^{n_{ji}},$$

with $n_{ji} = e_{L/M}(\mathfrak{P}_{ji}) f_{L/M}(\mathfrak{P}_{ji})$ by Theorem 5.11 (i), and so, using Theorem 4.5, we arrive at the equality

$$\prod_{j=1}^{k_i} N_{L_{\mathfrak{P}_{ji}}/M_{\mathfrak{Q}_i}}(x) = x^{[L:M]},$$

which gives

$$\prod_{i=1}^{s}\prod_{j=1}^{k_i} N_{L_{\mathfrak{P}_{ji}}/K_{\mathfrak{p}}}(x) = \prod_{i=1}^{s}\prod_{j=1}^{k_i} N_{M_{\Omega_i}/K_{\mathfrak{p}}}(N_{L_{\mathfrak{P}_{ji}}/M_{\Omega_i}}(x))$$
$$= \prod_{i=1}^{s}\left(N_{M_{\Omega_i}/K_{\mathfrak{p}}}(x)\right)^{[L:M]} = N_{L/K}(x),$$

as required. A similar argument, in which products are replaced by sums and exponents by coefficients, applies to traces. □

2. In this subsection we shall consider connections between the different of an extension of an algebraic number field and the corresponding local differents.

Proposition 6.2. *For every finite extension L/K of algebraic number fields one has*

$$D_{L/K} = \prod_{\mathfrak{P}} \left(D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \cap R_L\right),$$

where the product is taken over all prime ideals $\mathfrak{P}$ of R_L, and $\mathfrak{p}$ denotes the prime ideal of R_K, lying below $\mathfrak{P}$.

Proof : The assertion results immediately from the following lemma:

Lemma 6.3. *If $\mathfrak{P}$ lies above $\mathfrak{p}$, then*

$$D_{L/K} = \mathfrak{P}^k \mathfrak{I},$$

where $\mathfrak{I}$ is an ideal of R_L not divisible by $\mathfrak{P}$, and $\mathfrak{P}^k R_{L_{\mathfrak{P}}}$ is the different of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Proof : Let $\mathfrak{P}^r \parallel D_{L/K}$, and after identifying the prime ideal of $L_{\mathfrak{P}}$ with $\mathfrak{P}$ write $D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathfrak{P}^k$. By Theorem 4.16 there exists $a \in R_L$ such that if F is its minimal polynomial over R_K, then $F'(a) \in \mathfrak{P}^r \setminus \mathfrak{P}^{r+1}$. If $F = F_1 \cdots F_t$ is the factorization of F into monic factors irreducible over $K_{\mathfrak{p}}$, having coefficients in R, then for a certain i we have $F_i(a) = 0$, and obviously $L_{\mathfrak{P}} = K_{\mathfrak{p}}(a)$. Differentiating, we get $F'(a) = F_i'(a)G(a)$ with a certain polynomial $G \in R[X]$, whence, using the fact that $F_i'(a)$ generates the different $D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, we obtain $r \geq k$. Assume that r exceeds k. According to Theorem 4.22 there exists an essential derivation $d : S \longrightarrow S/\mathfrak{P}^{k+1}$, vanishing on R. Since its restriction to R_L is also a derivation $d^* : R_L \longrightarrow R_L/\mathfrak{P}^{k+1}$, vanishing on R_K, the same theorem implies that it is not essential, i.e., every element of its image $d^*(R_L)$ is a zero-divisor. This leads to a contradiction. Indeed, let A be the set of all elements $a \in S$ for which $d(a)$ is a zero-divisor. Lemma 4.23 shows that d is continuous, and since $S/\mathfrak{P}^{k+1}$ is finite, the set A must be closed. But it contains R_L, and therefore must coincide with S, thus d is not essential, contradiction. □

The proposition follows by considering separately all prime ideals dividing $D_{L/K}$, and applying the lemma. □

Corollary 1. *A prime ideal $\mathfrak{P}$ of R_L is unramified or tamely ramified in L/K if and only if the corresponding $\mathfrak{p}$-adic extension is unramified or tame.*

Proof : This follows from the proposition and Corollary 1 to Theorem 4.24. □

Corollary 2. *A prime ideal $\mathfrak{P}$ of R_L is wildly ramified in L/K if and only if one has $\mathfrak{P}^e | D_{L/K}$, where $e = e_{L/K}(\mathfrak{P})$.*

Proof : Apply the last proposition, Proposition 5.28 and Theorem 4.24. □

Corollary 3. *If L/K is normal, then the trace map $T_{L/K} : R_L \longrightarrow R_K$ is surjective if and only if L/K is tame.*

Proof : If L/K is tame, then the surjectivity of the trace map is contained in Corollary 5 to Theorem 4.24. If the trace map is surjective, $\mathfrak{P}$ is a wildly ramified prime ideal of R_L, and $\mathfrak{p} \subset R_K$ lies below $\mathfrak{P}$, then using Theorem 4.6 we obtain that all prime ideals $\mathfrak{P}_1 = \mathfrak{P}, \ldots, \mathfrak{P}_k$ lying above $\mathfrak{p}$ are wildly ramified, and if e is their common ramification index, then the preceding corollary implies $\mathfrak{p}R_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_k)^e | D_{L/K}$, contradicting Corollary 3 to Proposition 4.13. □

Observe that in the case of a non-normal extension the trace map can be surjective even if the extension is not tame. In fact, let $L/\mathbb{Q}$ be a cubic extension in which 3 is unramified and $2R_L = \mathfrak{P}_1^2\mathfrak{P}_2$. Then $\mathfrak{P}_1$ is the only wildly ramified prime ideal, because in view of Theorem 4.5 only prime divisors of $2R_L$ and $3R_L$ may ramify wildly in a cubic extension . Assume now that $T_{L/\mathbb{Q}}(R_L) \neq \mathbb{Z}$. Then by Corollary 2 to Proposition 4.13 there is a prime p such that if

$$pR_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

then for $i = 1, 2, \ldots, g$ one has $\mathfrak{P}_i^{e_i} | D_{L/K}$, and thus, by Theorem 4.24, all prime ideals $\mathfrak{P}_i$ must be wildly ramified. But in our case there is no such prime p, since $\mathfrak{P}_2$ is tame, whence $T_{L/\mathbb{Q}}$ is surjective.

To show that this situation can really occur, consider $L = \mathbb{Q}(a)$, where a is a root of the polynomial $X^3 + 15X^2 + 20X + 30$, which is irreducible, being Eisensteinian with respect to the prime 5. Proposition 2.9 (iv) easily leads to $|d_{L/\mathbb{Q}}(a)| = 2^2 \cdot 5^2 \cdot 13 \cdot 23$, thus 3 is unramified and 2 is ramified, hence we have only to exclude the possibility of $2R_L = \mathfrak{P}^3$. If this would happen, then Theorem 4.24 would imply $\mathfrak{P}^2 | D_{L/\mathbb{Q}}$, whence $2^2 = N(\mathfrak{P}^2) | d(L)$. In view

of $2^2 \parallel d_{L/\mathbb{Q}}(a)$ this shows that 2 does not divide the index of a, and thus Theorem 4.33 is applicable. Since

$$X^3 + 15X^2 + 20X + 30 \equiv X^3 + X^2 \equiv X^2(X+1) \pmod 2,$$

we obtain $2R_L = \mathfrak{P}_1^2\mathfrak{P}_2$, with $\mathfrak{P}_1 \neq \mathfrak{P}_2$, contrary to our assumption.

Corollary 4. *If* $[K_i : K] = n_i$ $(i = 1, 2)$ *and* $L = K_1K_2$, *then*

$$d(L/K) | d(K_1/K)^{n_2} d(K_2/K)^{n_1}.$$

Proof: Let $\mathfrak{P}$ be a prime ideal in R_L and $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2$ the prime ideals in R_K, R_{K_1}, R_{K_2}, lying below $\mathbb{P}$. Assume that $\mathfrak{p}_1^a \parallel D_{K_1/K}$, and consider the corresponding $\mathfrak{p}$-adic fields, putting $k_i = K_{i_{\mathfrak{p}_i}}$ for $i = 1, 2$. Then

$$D_{k_1/K_\mathfrak{p}} = \mathfrak{p}_1^a = \delta_{k_1/K_\mathfrak{p}}(c)S',$$

holds with a suitable $c \in S'$, S' being the ring of integers of k_1. Since $L = K_1K_2$, we have $L_\mathfrak{P} = k_1k_2$ and thus $L_\mathfrak{P} = k_2(c)$. If F and G are minimal polynomials of c over $K_\mathfrak{p}$ and k_2, respectively, then for a certain polynomial H with integral coefficients from k_2 we have $F(X) = G(X)H(X)$, which gives $F'(c) = G'(c)H(c)$, and we see that the different of $L_\mathfrak{P}/k_2$ divides the ideal generated by $F'(c)$, which equals $D_{k_1/K_\mathfrak{p}}S''$, with S'' being the ring of integers of $L_\mathfrak{P}$. Applying our proposition we obtain $D_{L/K_2} | D_{K_1/K}R_L$, hence

$$D_{L/K} = D_{L/K_2}D_{K_2/K} | D_{K_1/K}D_{K_2/K}R_L,$$

and taking norms we arrive at

$$\begin{aligned} d(L/K) &= N_{L/K}(D_{L/K}) | N_{L/K}(D_{K_1/K}R_L)N_{L/K}(D_{K_2/K}R_L) \\ &= d(K_1/K)^{[L:K_1]} d(K_2/K)^{[L:K_2]}. \end{aligned}$$

It suffices now to note that $[L : K_1] \leq n_2$ and $[L : K_2] \leq n_1$. □

Corollary 5. *There can be only finitely many extensions* $K/\mathbb{Q}$ *of a fixed degree* n, *having a prescribed finite set of ramified primes.*

Proof: In view of Theorem 2.24 and the last assertion of Proposition 4.14 it suffices to show that the discriminant of $K/\mathbb{Q}$ can attain only a finite number of distinct values. Since the degrees of local extensions $K_\mathfrak{p}/\mathbb{Q}_p$ are divisors of n, this is a consequence of the proposition and Corollary 2 to Theorem 5.27. □

Finally we prove a bound for the maximal power of a prime ideal which can divide the different, generalizing the second part of Theorem 4.24 to wildly ramified prime ideals:

Proposition 6.4. *If* $\mathfrak{p}R_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ *with distinct* $\mathfrak{P}_i$, *then the different* $D_{L/K}$ *cannot be divisible by* $\mathfrak{P}_i^{e_i+s_i}$, *where* s_i *is the maximal power of* $\mathfrak{P}_i$, *dividing* $e_i R_L$.

Proof : By Proposition 6.2 it suffices to prove the result for the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, where $\mathfrak{P}$ is one of the $\mathfrak{P}_i$'s. If M is the maximal unramified extension of $K_{\mathfrak{p}}$, contained in $L_{\mathfrak{P}}$, then $e(L_{\mathfrak{P}}/M) = e_i$, and $L_{\mathfrak{P}}/M$ is fully ramified. Using Theorem 5.27 we can write $L_{\mathfrak{P}} = M(\pi)$, where π generates $\mathfrak{P}$, and is a root of an Eisensteinian polynomial $F(X) = X^{e_i} + \cdots + a_{e_i} \in M[X]$ such that the different of $L_{\mathfrak{P}}/M$ is generated by $F'(\pi)$. Denoting by ν the exponent corresponding to $\mathfrak{P}$ in $L_{\mathfrak{P}}$, we see that for $r = 1, 2, \ldots, e_i - 1$ we have

$$\nu(a_r(e_i - r)\pi^{e_i - r - 1}) \equiv -(r+1) \pmod{e_i},$$

because $\nu(a_r)$ and $\nu(e_i - r)$ are divisible by e_i. Hence all summands in the sum

$$F'(\pi) = e_i\pi^{e_i-1} + a_1(e_i - 1)\pi^{e_i-2} + \cdots + a_{e_i-1}$$

give distinct values to the exponent ν, and since the first summand gives

$$\nu(e_i\pi^{e_i-1}) = s_i + e_i - 1,$$

the different cannot be divisible by a higher power of $\mathfrak{P}$ than $\mathfrak{P}^{s_i+e_i-1}$. □

3. If the extension L/K is normal, then it is possible to apply the theory of ramification groups, developed for $\mathfrak{p}$-adic fields in Chap. 5, and, in particular, to defined the ramification groups of such an extension.

Theorem 6.5. *If* L/K *is a normal extension of an algebraic number field,* G *is its Galois group,* $\mathfrak{p}$ *is a prime ideal of* R_K, *and* $\mathfrak{P}$ *is a prime ideal of* R_L *lying above* $\mathfrak{p}$, *then the corresponding extension* $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ *of* $\mathfrak{p}$*-adic fields is normal, and there is a canonical embedding of* $\mathfrak{G} = Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ *into* G. *The index of the image of* $\mathfrak{G}$ *in* G *equals the number of prime ideals lying above* $\mathfrak{p}$ *in* L.

Proof : Write $L_{\mathfrak{P}} = K_{\mathfrak{p}}(a)$, where a is a generator of the extension L/K. The conjugates of a over $K_{\mathfrak{p}}$ form a subset of the set of conjugates of a over K, and so they all lie in $L \subset L_{\mathfrak{P}}$, whence the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is normal. The same observation shows that the restriction of $\sigma \in \mathfrak{G}$ to L is an element of G, and this gives a homomorphism $\phi : \mathfrak{G} \longrightarrow G$, which is injective, because if $\phi(\sigma)$ is the identity map, then $\sigma(a) = a$, and therefore σ is the identity map on the whole field $L_{\mathfrak{P}}$. By Theorem 5.11 (i) the group $\mathfrak{G}$ has $e_{L/K}(\mathfrak{P})f_{L/K}(\mathfrak{P})$ elements, hence an application of Theorem 4.6 proves the last assertion. □

The image of $\mathfrak{G}$ in G is called the *decomposition group* of the ideal $\mathfrak{P}$. In the sequel we shall identify it with $\mathfrak{G}$, and this convention implies that we can

regard the inertia group and ramification groups of the corresponding local extension as subgroups of G. These subgroups are called the *inertia group*, respectively the *ramification groups* of $\mathfrak{P}$. They were originally defined by Hilbert [94a] without the use of $\mathfrak{p}$-adic fields. Our next proposition shows the equivalence of Hilbert's definition with the one given above.

Proposition 6.6. *Let L/K be a normal extension of an algebraic number field K, let G be its Galois group, and let $\mathfrak{P}$ be a prime ideal of R_L. If we define a sequence $G_{-1}(\mathfrak{P})$, $G_0(\mathfrak{P})$, $G_1(\mathfrak{P})$,... of subgroups of G by*

$$G_{-1}(\mathfrak{P}) = \{g \in G : \ g(\mathfrak{P}) = \mathfrak{P}\},$$

$$G_i(\mathfrak{P}) = \{g \in G : \ g(x) - x \in \mathfrak{P}^{i+1} \text{ for } x \in R_L\} \quad (i = 0, 1, \ldots),$$

then $G_{-1}(\mathfrak{P})$ equals the decomposition group of $\mathfrak{P}$, $G_0(\mathfrak{P})$ is its inertia group and, for $i \geq 1$, $G_i(\mathfrak{P})$ is its i-th ramification group.

Proof: Let $\mathfrak{p}$ be the prime ideal of R_K lying below $\mathfrak{P}$, and denote by S the ring of integers of $L_{\mathfrak{P}}$. Observe that every element g of the decomposition group fixes the ideal $\mathfrak{P}$. Indeed, we can write $g = \bar{g}_{|L}$, where $\bar{g}$ is an automorphism of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, and this gives

$$\bar{g}(\mathfrak{P}S) = \mathfrak{P}S$$

and

$$g(\mathfrak{P}) = \bar{g}(\mathfrak{P}) = \bar{g}(\mathfrak{P}S \cap R_L) \subset \mathfrak{P}S \cap R_L = \mathfrak{P}.$$

But $g(\mathfrak{P})$ is a prime ideal, and therefore the equality $g(\mathfrak{P}) = \mathfrak{P}$ follows, showing that the decomposition group of $\mathfrak{P}$ is a subgroup of $G_{-1}(\mathfrak{P})$. Now note that these two groups are of the same order. In fact, the cosets of G with respect to $G_{-1}(\mathfrak{P})$ consist of elements mapping $\mathfrak{P}$ onto a fixed prime ideal conjugated to $\mathfrak{P}$, and so the index $[G : G_{-1}(\mathfrak{P})]$ equals the number of such ideals. It remains to apply the last part of Theorem 6.5 to obtain the equality of $G_{-1}(\mathfrak{P})$ and the decomposition group.

Now let us look at the remaining groups from our sequence. It follows directly from the definitions that the inertia group of $\mathfrak{P}$ is contained in $G_0(\mathfrak{P})$ and the i-th ramification group is contained in $G_i(\mathfrak{P})$. To prove that we have equalities here, note that by Corollary 2 to Proposition 5.7 every element of $\mathfrak{G} = Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is continuous. Let $g \in G_i$, and assume that g is the restriction to L of $\bar{g} \in \mathfrak{G}$. If $a \in S$, then a is the limit of a sequence $\{a_n\}$ of elements of R_L, and since $\mathfrak{P}^{i+1}$ is open we get $a_n \in a + \mathfrak{P}^{i+1}$ for n sufficiently large. By our assumption $g(a_n) - a_n \in \mathfrak{P}^{i+1}$, hence for large n we get $g(a_n) \in a + \mathfrak{P}^{i+1}$. Since the coset $a + \mathfrak{P}^{i+1}$ is closed, it contains $\lim_n g(a_n) = \lim_n \bar{g}(a_n) = \bar{g}(a)$, thus $\bar{g}(a) - a$ lies in $\mathfrak{P}^{i+1}$, and this implies our assertion. □

Lemma 6.7. *If L/K is a normal extension of an algebraic number field K, M is a subfield of L containing K, and $H = Gal(L/M)$ is the subgroup*

of the Galois group of L/K corresponding to M, then for $i = -1, 0, 1, \ldots$ the subgroup G_i of H, corresponding to the prime ideal $\mathfrak{P} \subset R_L$, equals the intersection of H with the subgroup $G_i(\mathfrak{P})$ of $Gal(L/K)$.

Proof : Immediate by the definition of the groups G_i. □

The field corresponding by Galois theory to the decomposition group of $\mathfrak{P}$ will be denoted by $K_{-1}(\mathfrak{P})$ and called the *decomposition field* or the *splitting field* of $\mathfrak{P}$. Similarly, the fields corresponding to the inertia group and the i-th ramification group will be denoted by K_0 and K_i, respectively, and called the *inertia field* and the i-th *ramification field* of $\mathfrak{P}$. The next proposition describes the main properties of these fields:

Proposition 6.8. *Let L/K be a normal extension of algebraic number fields, fix a prime ideal $\mathfrak{P}$ of R_L, let $\mathfrak{p}$ be the prime ideal of R_K lying below $\mathfrak{P}$, denote by $\mathfrak{P}_i$ $(i = -1, 0, 1, \ldots)$ the prime ideal of R_{K_i} lying below $\mathfrak{P}$, and let p be the rational prime lying in $\mathfrak{p}$. Moreover, write $e = e_{L/K}(\mathfrak{P}) = e_0 p^m$ with $p \nmid e_0$ and $f = f_{L/K}(\mathfrak{P})$.*

(i) In the decomposition field K_{-1} we have $\mathfrak{p}R_{K_{-1}} = \mathfrak{P}_{-1}\mathfrak{I}$, with $\mathfrak{P}_{-1} \nmid \mathfrak{I}$ and $f_{K_{-1}/K}(\mathfrak{P}_{-1}) = 1$. Moreover, K_{-1} is the maximal subfield of L having these properties.

(ii) In the inertia field K_0 we have $\mathfrak{p}R_{K_0} = \mathfrak{P}_0\mathfrak{I}_0$, with $\mathfrak{P}_0 \nmid \mathfrak{I}_0$ and $f_{K_0/K}(\mathfrak{P}_0) = f$. Moreover, K_0 is the maximal subfield of L having these properties.

(iii) In the first ramification field K_1 we have $\mathfrak{p}R_{K_1} = \mathfrak{P}_1^{e_0}\mathfrak{I}_1$, with $\mathfrak{P}_1 \nmid \mathfrak{I}_1$ and $f_{K_1/K}(\mathfrak{P}_1) = f$. Moreover, K_1 is the maximal subfield of L having these properties.

(iv) The extension K_0/K_{-1} is cyclic of degree f, K_1/K_0 is cyclic of degree e_0, and L/K_1 is a p-extension of degree p^m.

Proof : Clearly $K_{\mathfrak{p}} \subset (K_{-1})_{\mathfrak{P}_{-1}} \subset L_{\mathfrak{P}}$, and since the Galois group of the extension $L_{\mathfrak{P}}/L_{\mathfrak{p}}$ fixes K_{-1}, it must fix, by continuity, also its closure $(K_{-1})_{\mathfrak{P}_{-1}} = K_{\mathfrak{p}}$. In turn we obtain, by Theorem 5.11 the equalities

$$e_{K_{-1}/K}(\mathfrak{P}_{-1}) = f_{K_{-1}/K}(\mathfrak{P}_{-1}) = 1,$$

and so $\mathfrak{p}R_{K_{-1}} = \mathfrak{P}_{-1}\mathfrak{I}$, with $\mathfrak{P}_{-1} \nmid \mathfrak{I}$. Moreover, if M is a field with $K \subset M \subset L$, and for the prime ideal $\mathfrak{P}_M$ of R_M, lying below $\mathfrak{P}$ we have $e_{M/K}(\mathfrak{P}_M) = f_{M/K}(\mathfrak{P}_M) = 1$, then $M_{\mathfrak{P}_M} = K_{\mathfrak{p}}$ and M is fixed by G_{-1}, implying $M \subset K_{-1}$. This establishes (i), and the remaining assertions are immediate by Theorems 5.11, 5.34 and the definition of the groups G_i. □

Corollary 1. *If L/K is a normal extension of an algebraic number field K, $\mathfrak{P}$ is a prime ideal of R_L, and $\mathfrak{p} \subset R_K$ lies below $\mathfrak{P}$, then*

$$e_{L/K}(\mathfrak{P}) = \#G_0(\mathfrak{P}), \text{ and } f_{L/K}(\mathfrak{P})e_{L/K}(\mathfrak{P}) = \#G_{-1}(\mathfrak{P}).$$

Proof : Follows immediately from the proposition. □

The next result is sometimes called the *monodromy theorem* for algebraic number fields:

Corollary 2. *Let L/K be a normal finite extension of an algebraic number field, and let G be its Galois group. The subgroup H of G generated by all inertia groups of prime ideals of R_L corresponds to the maximal subfield of L, unramified over K. In particular, if $K = \mathbb{Q}$, then the inertia groups of all prime ideals of R_K generate G.*

Proof : Let M be the subfield of L, corresponding to H and let M_0 be the maximal subfield of L, unramified over K. By Lemma 6.7 and the preceding corollary we have

$$e_{M/K}(\mathfrak{P} \cap R_M) = \#G_0(\mathfrak{P})/\#(G_0(\mathfrak{P}) \cap H) = 1,$$

as $G_0(\mathfrak{P}) \cap H = G_0(\mathfrak{P})$. This shows that no prime ideal ramifies in M/K, and therefore $M \subset M_0$. Conversely, if M_1 is a subfield of L unramified over K, and H_1 is the corresponding subgroup of G, then for every prime ideal $\mathfrak{P}$ of L we have $G_0(\mathfrak{P}) = G_0(\mathfrak{P}) \cap H_1$, thus $G_0(\mathfrak{P}) \subset H_1$ and $H \subset H_1$, implying $M1 \subset M$. In particular we obtain $M_0 \subset M$.

If $K = \mathbb{Q}$, then by Corollary 4 to Theorem 4.24 we have $H = G$. □

Corollary 1 shows that in a normal extension the sequences $G_i(\mathfrak{P})$ determine the decomposition of prime ideals. It follows from Lemma 6.7 that these sequences determine also the decomposition in all subfields of L containing K.

We conclude this subsection with the determination of the maximal power of a prime ideal, dividing the different of a normal extension:

Proposition 6.9. *If L/K is a normal extension of an algebraic number field K, and $\mathfrak{P}$ is a prime ideal of R_L, then its maximal power dividing $D_{L/K}$ equals $\mathfrak{P}^A$ with*

$$A = A(\mathfrak{P}) = \sum_{i=0}^{t} (\#G_i(\mathfrak{P}) - 1),$$

where t is the maximal index for which the group $G_i(\mathfrak{P})$ is non-trivial. Conjugated prime ideals have the same value of $A(\mathfrak{P})$.

Proof : The first assertion results from Proposition 6.2 and Theorem 5.36, and the second is a consequence of the simple observation that conjugated prime ideals have conjugated corresponding groups G_i. □

Corollary 1. *If L/K is normal of odd degree n, and T_n is the greatest common divisor of all numbers $(p-1)/2$ for prime $p|n$, then $d(L/K)$ is a $2T_n$-th power of an ideal of R_L.*

Proof : Let $\mathfrak{p}$ be a prime ideal of R_K ramified in L/K, and let $\mathfrak{p}R_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$. The proposition implies $\mathfrak{p}^B \parallel d(L/K) = N_{L/K}(D_{L/K})$ with $B = rfA$, where $f = f_{L/K}(\mathfrak{P}_1)$ and $A = A(\mathfrak{P}_1)$, because the prime ideals $\mathfrak{P}_i$ are all conjugated. The assertion will be established, if we would show that for all prime ideals $\mathfrak{P}$ of R_L we have $2T_n|A(\mathfrak{P})$. Since e divides n, every its prime divisor is congruent to unity mod $2T_n$, hence $e \equiv 1 \pmod{2T_n}$, leading to

$$\#G_0(\mathfrak{P}) \equiv 1 \pmod{2T_n}$$

by Corollary 1 to Proposition 6.8. If $G_1(\mathfrak{P})$ is trivial, then $A(\mathfrak{P}) = \#G_0(\mathfrak{P}) - 1$, and we get $2T_n|A(\mathfrak{P})$. If $G_1(\mathfrak{P})$ is non-trivial, then the rational prime p lying below $\mathfrak{P}$ divides e, hence $p|n$. By Proposition 6.8 and Corollary 2 to Theorem 5.34 all ramification groups are p-groups, thus for $i \geq 1$ we get $\#G_i(\mathfrak{P}) \equiv 1 \pmod{p-1}$, but in view of $p|n$ we have $2T_n|p-1$ and we conclude that also in this case $2T_n$ divides $A(\mathfrak{P})$. □

Corollary 2. *If L/K is a normal extension of a prime degree q, then $d(L/K)$ is a $(q-1)$st power of an ideal of R_K.*

Proof : This is a special case of Corollary 1. □

4. In this subsection we shall consider certain properties of characters mod I for ideals I. These properties will be later utilized in the theory of Gaussian sums.

Let us start with definitions. Let K be an algebraic number field, and let I be a non-zero ideal of R_K. Denote by $G(I)$ the multiplicative group of residue classes mod I which are relatively prime to I, and let χ be a character of that group. It is customary to treat this character as a function defined for all integers of K by means of the formula

$$\chi(a) = \begin{cases} \chi(a \bmod I) & \text{if } a \bmod I \in G(I), \\ 0 & \text{otherwise.} \end{cases}$$

Observe that the function so defined has the multiplicative property, but it is not a group character in the usual sense.

In the case when K is the field of rational numbers we shall write, for simplicity, $G(N)$ instead of $G(N\mathbb{Z})$, assuming always that N is the positive generator of the ideal $N\mathbb{Z}$.

A character χ of $G(I)$ is called *primitive*, if there is no ideal $J \neq I$, dividing I with the property that from $(xR_K, I) = 1$ and $x \equiv 1 \pmod{J}$ the equality $\chi(x) = 1$ follows. It is obvious that if I is a prime ideal, then every non-trivial character of $G(I)$ is primitive, and the trivial character is

primitive only if $I = R_K$. Observe, moreover, that every character χ of $G(I)$ can be regarded as a primitive character of $G(J)$, J being a suitable divisor of I. Indeed, let J be the greatest common divisor of all ideals I_0 dividing I for which χ is trivial on the residue class 1 mod I_0. Then one sees easily, as in the rational case, that χ equals unity on the residue class 1 mod J. Therefore it induces a character χ' of $G(J)$, and the ideal J is called the *conductor* of χ. The character χ' is clearly a primitive character of $G(J)$. It is called the *primitive character induced by* χ. In the case $K = \mathbb{Q}$ it is customary to regard the unique positive generator of J as the *conductor* of χ. Clearly no confusion can arise here.

For every χ of $G(I)$ we have $\chi^2(-1) = 1$, whence $\chi(-1) = \pm 1$. Characters χ satisfying $\chi(-1) = 1$ are called *even characters*, and the remaining characters are called *odd*.

Corollary 3 to Proposition 1.14 shows that if $I = I_1 \cdots I_r$ is a factorization of I into factors pairwise relatively prime, then we have also a factorization $G(I) = G(I_1) \times \cdots \times G(I_r)$ of corresponding groups. Thus every character χ of $G(I)$ can be written as a product of characters of $G(I_j)$, since if we put $\chi_i(x \bmod I_i) = \chi(u)$, where $u \equiv x \,(\mathrm{mod}\, I_i)$ and $u \equiv 1 \,(\mathrm{mod}\, I/I_i)$, then

$$\chi(x \bmod I) = \prod_{i=1}^{r} \chi_i(x \bmod I_i). \tag{6.1}$$

Proposition 6.10. *If χ is a character of $G(I)$, and $I = \prod_{i=1}^{r} I_i$ is a factorization into pairwise co-prime factors, then χ is primitive if and only if every factor χ_i in the factorization* (6.1) *is primitive.*

Proof : Let J_i be the conductor of χ_i for $i = 1, 2, \ldots, r$ and put $J = \prod_{i=1}^{r} J_i$. Then for $x \equiv 1 \,(\mathrm{mod}\, J)$, satisfying $(xRK, I) = 1$, we have $\chi(x) = \prod_{i=1}^{r} \chi_i(x) = 1$. It follows that if a factor χ_i is not primitive, then $I_i \neq J_i$, hence $J \neq I$, and χ is not primitive.

Conversely, if χ is not primitive, say $\chi(x) = 1$ holds for $x \equiv 1 \,(\mathrm{mod}\, \mathfrak{J})$ with a certain $\mathfrak{J} | I$, $\mathfrak{J} \neq I$, then $\mathfrak{J} = \prod_{i=1}^{r} \mathfrak{J}_i$ with $\mathfrak{J}_i | I_i$ and therefore there exists i with $I_i \neq \mathfrak{J}_i$. But then for $x \equiv 1 \,(\mathrm{mod}\, \mathfrak{J}_i)$ we have $\chi_i(x) = 1$, showing that χ_i is not primitive. □

To determine the characters of $G(I)$ one has to know the structure of this group. In particular, it is important to know in which cases $G(I)$ is cyclic. If this happens, then every its generator is called a *primitive root* mod I. In the case of the field of rational numbers it is a classical result that the multiplicative group of residue classes mod M, prime to M, is cyclic if and only if either M is a power of an odd prime, or it is a double of such power, or finally $M = 1, 2, 4$. In the general case things become more complicated, so we shall consider only the case of prime ideal powers. The corresponding assertion in the general case can be obtained from this result by noting that

a product of cyclic groups is cyclic if and only if their orders are pairwise relatively prime. We leave the tedious but not difficult computation to the interested reader.

Theorem 6.11. *Let $I = \mathfrak{P}^N$ be a power of a prime ideal. The group $G(I)$ is cyclic if and only if one the following cases holds:*

(i) $I = \mathfrak{P}$,

(ii) $I = \mathfrak{P}^2$, and $f_{K/\mathbb{Q}}(\mathfrak{P}) = 1$,

(iii) $I = \mathfrak{P}^N$, where $N \geq 3$, $2 \notin \mathfrak{P}$, and $e_{K/\mathbb{Q}}(\mathfrak{P}) = f_{K/\mathbb{Q}}(\mathfrak{P}) = 1$, i.e. the corresponding local extension is trivial,

(iv) $I = \mathfrak{P}^3$, $2 \in \mathfrak{P}$, $f_{K/\mathbb{Q}}(\mathfrak{P}) = 1$, and $e_{K/\mathbb{Q}}(\mathfrak{P}) \geq 2$.

Proof : We begin with a simple lemma, translating the whole problem into the language of $\mathfrak{p}$-adic fields:

Lemma 6.12. *For any prime ideal $\mathfrak{P}$ and $N \geq 1$ the group $G(\mathfrak{P}^N)$ is isomorphic with the factor group $U(K_{\mathfrak{P}})/U_N(K_{\mathfrak{P}})$.*

Proof : Apply Proposition 5.17 (iii) and Corollary 1 to Theorem 5.2. □

Put $U = U(K_{\mathfrak{P}})$, $U_N = U_N(K_{\mathfrak{P}})$, choose $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, and let p be the rational prime contained in $\mathfrak{P}$. The case (i) is trivial, as $G(I) = (R_K/\mathfrak{P})^*$ is the multiplicative group of a finite field, hence is cyclic.

If $N \geq 2$ and U/U_N is cyclic, then U_1/U_2 is also cyclic, but Corollary to Proposition 5.17 and Theorem 5.11 (iv) show that U_1/U_2 can be cyclic only if $f_{K/Q}(\mathfrak{P}) = 1$. If the last condition is satisfied, then $U_1/U_2 \sim C_p$ and since $U/U_1 \sim C_{p-1}$ we obtain $G(\mathfrak{P}^2) \sim U/U_2 \sim C_{p(p-1)}$, in view of $(p, p-1) = 1$. This settles (ii).

Since we know already that in the case $f_{K/\mathbb{Q}}(\mathfrak{P}) \geq 2$ the group $G(\mathfrak{P}^N)$ can be cyclic only for $N = 1$, we may assume that $f_{K/\mathbb{Q}}(\mathfrak{P}) = 1$ holds. Since for $a \in K_{\mathfrak{P}}$ we have

$$(1 + \pi a)^p = 1 + p\pi a + \cdots + p\pi^{p-1}a^{p-1} + \pi^p a^p,$$

we see that the map $x \mapsto x^p$ maps U_1 into U_r with $r = \min\{p, 1+e\}$, whence the group U_1/U_r can be cyclic only if $r = 2$, because in the remaining cases all its elements have order p. Now observe that the case $r = 2$ arises if either $p = 2$ or $e = 1$.

If $e = 1$, then $K_{\mathfrak{P}} = \mathbb{Q}_p$, thus the group $G(\mathfrak{P}^N) \sim G(p^N)$ is cyclic for all odd primes p and $N \geq 1$, whereas it is non-cyclic if $p = 2$ and $N \geq 3$. This settles (iii).

If $p = 2$ and $e \geq 2$, then in view of $(1 + \pi)^2 = 1 + \pi^2 + 2\pi \in U_2 \setminus U_3$ we obtain that the group U_1/U_3 is generated by $1 + \pi$, thus is cyclic, and the group U_1/U_4 is non-cyclic because every its element is of order not exceeding 4, due to

$$(1+\pi a)^4 = 1 + 4\pi a + 6\pi^2 a^2 + 4\pi^3 a^3 + \pi^4 a^4 \in U_4,$$

whereas $\#U_1/U_4 = 8$. Since in this case we have $U = U_1$, (iv) follows. □

Lemma 6.12 shows that every character of $G(\mathfrak{P}^N)$ is in fact a character of the factor group $U(K_\mathfrak{P})/U_N(K_\mathfrak{P})$, and one sees that the two definitions of the conductor of a character, which we have at this moment, are in perfect agreement.

We conclude this subsection with the determination of ideals I for which the group $G(I)$ has a real primitive character, i.e., a primitive character assuming the values 1 and -1 exclusively.

Proposition 6.13. *The group $G(I)$ has a primitive real character if and only if*

$$I = \mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{Q}_1^{a_1} \cdots \mathfrak{Q}_s^{a_s},$$

where $\mathfrak{P}_i$ are distinct prime ideals not containing 2, $\mathfrak{Q}_i$ are distinct prime ideals containing 2, and $a_i \in \{0, 2, 4, \ldots, 2e_i, 1 + 2e_i\}$, with $e_i = e_{K/\mathbb{Q}}(\mathfrak{Q}_i)$ $(i = 1, 2, \ldots, s)$.

Proof : Proposition 6.10 permits us to restrict our attention to powers of prime ideals, so let $I = \mathfrak{P}^N$, and put $G = G(\mathfrak{P}^N)$.

Assume first that $2 \notin \mathfrak{P}$ and let χ be a real character of G. It will be convenient to treat χ as a character of U/U_N, which is permitted by Lemma 6.12. Since χ is real, we get $\chi(x^2) = \chi^2(x) = 1$ for $x \in G$, thus χ is trivial on squares. We have also

$$U/U_N \sim U/U_1 \times U_1/U_N,$$

because the orders of U/U_1 and U_1/U_N are relatively prime. Since every element of U_1 is a square, the number $1/2$ being integral in $K_\mathfrak{P}$, we see that χ is trivial on U_1/U_N, thus its conductor equals either $\mathfrak{P}$ or $\mathfrak{P}^0$. This shows that if $2 \notin \mathfrak{P}$, then only $G(\mathfrak{P})$ can have a primitive real character, and indeed it has one, because it is cyclic.

Now let us assume that $2 \in \mathfrak{P}$. If χ is a real character of G, then again χ is trivial on squares. By the Corollary to Lemma 5.19 the map $x \mapsto x^2$ maps U_{1+e} onto U_{1+2e}, hence our character has to be trivial on U_{1+2e}, and finally we find that there are no real primitive characters for $N \geq 2(1+e)$. Hence assume $1 \leq N \leq 2e+1$. Now observe that since the group U/U_1 is of odd order, the group $G \sim U/U_N$ will have a primitive real character if and only if there is a real character of $V_1 = U_1/U_N$, which is non-trivial on $V_2 = U_{N-1}/U_N$. Since the kernel of a non-trivial character is of index 2, and every subgroup of index 2 induces such a character, this will happen if and only if there is a subgroup of index 2 in V_1, which does not contain V_2, i.e., V_2 is not contained in the intersection A of all subgroups of index 2 of V_1. Note

now that A consists of all squares of elements of V_1. Indeed, V_1 is a product of cyclic 2-groups

$$V_1 = \prod_{i=1}^{t} C_{m_i}$$

with $m_i = 2^{s_i}$, $s_i \geq 1$ $(i = 1, 2, \ldots, t)$. If $x = [x_1, \ldots, x_t] \in A$ $(x_i \in C_{m_i})$, then x lies in every subgroup

$$V_1^{(j)} = \left(\prod_{i \neq j} C_{m_i} \right) \times C_j',$$

where C_j' is the group generated by y_j^2, where y_j is a generator of C_{m_j}. This implies that for every j the element x_j is a square, and thus x must be a square. Conversely, every square evidently lies in A.

Let now $N \leq 2e - 1$ be odd. If π generates $\mathfrak{P}$, $1 + c\pi^{N-1}$ is an arbitrary element of U_{N-1}, and a satisfies $a^2 \equiv c \pmod{\mathfrak{P}}$ (this congruence has solutions because $\#G(\mathfrak{P})$ is odd in view of $2 \in \mathfrak{P}$), then

$$1 + c\pi^{N-1} \equiv 1 + a^2\pi^{N-1} \pmod{\mathfrak{P}^N},$$

and in view of

$$2a\pi^{(N-1)/2} \equiv 0 \pmod{\mathfrak{P}^{e+(N-1)/2}}$$

and $e + (N-1)/2 \geq N$ we obtain

$$1 + c\pi^{N-1} \equiv \left(1 + a\pi^{(N-1)/2}\right)^2 \pmod{\mathfrak{P}^N},$$

i.e., $V_2 \subset A$, showing that in this case there is no primitive character mod $\mathfrak{P}^N$.

If $1 \leq N \leq 2e$ and N is even, then the image of $1 + \pi^{N-1}$ in V_2 does not lie in A. In fact, otherwise we would have

$$1 + \pi^{N-1} \equiv (1 + u\pi^M)^2 \pmod{\mathfrak{P}^N},$$

with a certain unit u and $M \geq 0$, thus if we define u_1 by $2 = u_1\pi^e$, then

$$1 + \pi^{N-1} \equiv 1 + uu_1\pi^{M+e} + u^2\pi^{2M} \pmod{\mathfrak{P}^N}.$$

If $M \geq e$, then this gives $1 + \pi^{N-1} \equiv 1 \pmod{\mathfrak{P}^{2e}}$, hence $2e \leq N-1$, contrary to our assumption. If, however, $M < e$, then

$$1 + \pi^{N-1} \equiv 1 + \pi^{2M}(u^2 + uu_1\pi^{e-M}) \pmod{\mathfrak{P}^N},$$

which leads to $N - 1 = 2M$, which is not possible, as $N - 1$ is odd. This establishes the existence of primitive real characters for $N = 0, 2, 4, \ldots, 2e$.

There remains the case $N = 1 + 2e$. Assume that every element of V_2 is a square. In particular, for every unit a the element $\alpha = 1 + a\pi^{2e}$ is a square

mod U_{1+2e} of a principal unit $1 + b\pi$. Writing $b = \epsilon\pi^n$ and $2 = \epsilon_1\pi^e$ with units ϵ, ϵ_1 and $n \geq 0$ we obtain

$$\alpha \equiv 1 + 2\pi b + \pi^2 b^2 \equiv 1 + \epsilon\epsilon_1\pi^{1+e+n} + \epsilon^2\pi^{2n+2} \pmod{\mathfrak{P}^{1+2e}}.$$

Now we distinguish three cases:

(i) $e - 1 < n$. In this case $\epsilon\epsilon_1\pi^{1+e+n}$ and $\epsilon^2\pi^{2n+2}$ both lie in $\mathfrak{P}^{1+2e}$, and hence α lies in U_{2e+1}, thus a cannot be a unit, contradiction.

(ii) $e - 1 > n$. In this case we have $\epsilon\epsilon_1\pi^{1+e+n} \in \mathfrak{P}^{2n+3}$, and therefore we obtain $2n + 2 = 2e$ and $n + 1 = e > n + 1$, again a contradiction.

(iii) $e - 1 = n$. Here we get $\alpha \equiv 1 + (\epsilon\epsilon_1 + \epsilon^2)\pi^{2e} \pmod{\mathfrak{P}^{1+2e}}$, hence $a \equiv \epsilon\epsilon_1 + \epsilon^2 \pmod{\mathfrak{P}}$, and wee see that if $\bar{\epsilon}_1 = \epsilon_1 \bmod \mathfrak{P}$, then the polynomial $F(X) = X^2 + \bar{\epsilon}_1 X$ maps the multiplicative group k^* of the field k of residue classes mod $\mathfrak{P}$ onto itself, i.e., for every non-zero $y \in k$ the polynomial $G(X) = F(X) + y$ is reducible in k. Writing $G(X) = (X - x_1)(X - x_2)$ we obtain $x_1 + x_2 = -\bar{\epsilon}_1$, $x_1 x_2 = y$. Since the map $F : k^* \longrightarrow k^*$ is surjective, and k^* is finite, hence F is injective, but this is not true in view of $F(x_1) = F(-x_1 - \bar{\epsilon}_1)$.

Hence there must be non-squares in V_2, and our proof is complete. □

5. Now we introduce Gaussian sums in algebraic number fields. They are intimately connected with the sums $\tau_0(\chi)$ considered in Chap. 5. In fact, in the most important case they will be equal, and in general our sums will be products of various sums $\tau_0(\chi)$.

Let K be an algebraic number field, $I \subset R_K$ a non-zero ideal, and let a be an element of the fractional ideal $\left(ID_{K/\mathbb{Q}}\right)^{-1}$. If χ is a character of $G(I)$, then the *Gaussian sum* $\tau_a(\chi)$, corresponding to the pair $[\chi, a]$ is defined by

$$\tau_a(\chi) = \sum_{x \bmod I} \chi(x) \exp(2\pi i T_{K/\mathbb{Q}}(ax)). \tag{6.2}$$

Observe that this sum does not depend on the choice of the system $x \bmod I$ of residues, because $x \equiv y \pmod{I}$ implies $\chi(x) = \chi(y)$, and since $T_{K/\mathbb{Q}}(ax) = T_{K/\mathbb{Q}}(ay) + T_{K/\mathbb{Q}}(a(x - y))$ and $a(x - y) \in D_{L/K}^{-1}$, Proposition 4.13 (iv) implies $T_{K/\mathbb{Q}}(a(x - y)) \in \mathbb{Z}$. and so $\exp(2\pi i T_{K/\mathbb{Q}}(ax)) = \exp(2\pi i T_{K/\mathbb{Q}}(ay))$.

In the special case $K = \mathbb{Q}$ we write $I = n\mathbb{Z}$, $a = k/n$ with suitable natural n and $a \in \mathbb{Z}$, and obtain the usual rational Gaussian sum

$$\tau_a(\chi) = \sum_{x \bmod n} \chi(x) \exp(2\pi i k x/n).$$

The case $k = 1$ is particularly important, and we shall denote the corresponding Gaussian sum simply by $\tau(\chi)$.

Proposition 6.14. *Let K be an algebraic number field, let I and χ be as above, and put $D = D_{K/\mathbb{Q}}$.*

(i) If b is an integer of K, prime to I, and $a \in (ID)^{-1}$, then $\tau_{ab}(\chi) = \overline{\chi(b)}\tau_a(\chi)$. In particular, if $K = \mathbb{Q}$, $I = n\mathbb{Z}$, $a = k/n$ with $(k,n) = 1$ and natural n, then $\tau_a(\chi) = \overline{\chi(k)}\tau(\chi)$.

(ii) Let $I = I_1 \cdots I_r$ be a factorization of an ideal I into factors pairwise relatively prime, let $\chi = \chi_1 \cdots \chi_r$ be the corresponding factorization of a character χ of $G(I)$, and put $J_i = I/I_i$. If $a \in (DI)^{-1}$ and for $i = 1, 2, \ldots, r$ the elements a_i belong to $(DI_i)^{-1}$, and satisfy $a - a_i \in (J_i D)^{-1}$, then

$$\tau_a(\chi) = \prod_{i=1}^{r} \tau_{a_i}(\chi_i).$$

(iii) One has

$$\tau_a(\bar{\chi}) = \chi(-1)\overline{\tau_a(\chi)}. \qquad \square$$

Proof : (i) Under our assumptions we have

$$\tau_{ab}(\chi) = \sum_{x \in G(I)} \chi(x) \exp(2\pi i T_{K/\mathbb{Q}}(abx)),$$

but if x runs over $G(I)$, then bx does the same, and we obtain

$$\tau_{ab}(\chi) = \overline{\chi(b)} \sum_{x \in G(I)} \chi(bx) \exp(2\pi i T_{K/\mathbb{Q}}(abx)) = \overline{\chi(b)}\tau_a(x).$$

(ii) For every $x \in R_K$, relatively prime to I, choose $x_i \in R_K$ with

$$x_i \equiv x \,(\mathrm{mod}\ I_i)$$

and

$$x_i \equiv 1 \,(\mathrm{mod}\ I_j) \quad (j \neq i).$$

Moreover let $y_1, \ldots, y_r$ be integers of K such that $y_i \equiv 1 \,(\mathrm{mod}\ I_i)$, and $y_i \in I_j$ for $j \neq i$. Then $\sum_{k=1}^{r} x_k y_k \equiv x \,(\mathrm{mod}\ I)$, and thus

$$\begin{aligned}
\tau_a(\chi) &= \sum_{x_1 \in G(I_1)} \cdots \sum_{x_r \in G(I_r)} \chi_1(x_1) \cdots \chi_r(x_r) \exp(2\pi i T_{K/\mathbb{Q}}(ax)) \\
&= \prod_{i=1}^{r} \sum_{x_i \in G(I_i)} \chi_i(x_i) \exp(2\pi i T_{K/\mathbb{Q}}(ax_i y_i)) \\
&= \prod_{i=1}^{r} \sum_{x_i \in G(I_i)} \chi_i(x_i) \exp(2\pi i T_{K/\mathbb{Q}}(a_i x_i y_i)),
\end{aligned}$$

since $ax_i y_i - a_i x_i y_i \in D^{-1}$, and the last product equals

$$\prod_{i=1}^{r} \tau_{a_i}(\chi_i),$$

because of (i) and $\chi_i(y_i) = 1$.

(iii) We have

$$\begin{aligned}
\tau_a(\overline{\chi}) &= \sum_{x \in G(I)} \overline{\chi(x)} \exp(2\pi i T_{K/\mathbb{Q}}(ax) \\
&= \sum_{x \in G(I)} \overline{\chi(x) \exp(2\pi i T_{K/\mathbb{Q}}(-ax)} \\
&= \chi(-1) \sum_{x \in G(I)} \overline{\chi(-x)} \exp(2\pi i T_{K/\mathbb{Q}}(ax) \\
&= \chi(-1)\overline{\tau_a(\chi)},
\end{aligned}$$

as asserted. □

Corollary. *Let $n = n_1 \cdots n_r$ be a factorization of a natural number n into mutually prime factors, let χ be a character of $G(n)$, and let $\chi = \chi_1 \cdots \chi_r$ be its factorization into characters of $G(n_i)$. Then*

$$\tau(\chi) = \prod_{i=1}^{r} \chi_i(n/n_i)\tau(\chi_i).$$

Proof : For $i = 1, 2, \ldots, r$ the congruence

$$xn/n_i \equiv 1 \pmod{n_i}$$

is solvable, so let b_i be one of its solutions. Then the numbers $a_i = b_i/n_i$ satisfy the assumptions of part (ii) of the proposition, whence

$$\tau(\chi) = \prod_{i=1}^{r} \tau_{a_i}(\chi_i).$$

Applying part (i) of the proposition we obtain $\tau_{a_i}(\chi) = \overline{\chi_i(b_i)}\tau(\chi_i)$, but in view of $b_i n/n_i \equiv 1 \pmod{n_i}$ we have $\overline{\chi_i(b_i)} = \chi_i(n/n_i)$, and this leads us to the asserted formula. □

The preceding proposition shows that the study of Gaussian sums corresponding to characters of $G(I)$ can be reduced to the case when I is a power of a prime ideal. We are mainly interested in Gaussian sums attached to primitive characters, and our next aim is to establish relations between them and the sums $\tau_0(\chi)$.

Proposition 6.15. *Let $\mathfrak{P}$ be a non-zero prime ideal of R_K, let $\mathfrak{P}_1 = \mathfrak{P}$, $\mathfrak{P}_2$, $\ldots$, $\mathfrak{P}_g$ be all prime ideals of R_K lying above $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$, and let χ be a primitive character of $G(\mathfrak{P}^N)$ $(N \geq 1)$. Fix $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, $\pi \notin \mathfrak{P}_j$ $(j = 2, 3, \ldots, g)$, and write $\pi R_K = \mathfrak{P}I$ $(\mathfrak{P} \nmid I)$ and $D_{K/\mathbb{Q}} = \mathfrak{P}^m J$ $(\mathfrak{P} \nmid J)$. Moreover choose $c \in R_K$ with $c \equiv 1 \pmod{\mathfrak{P}^N \mathfrak{P}_2 \cdots \mathfrak{P}_g}$ and $c \in I^{m+N}$, and put $a = c\pi^{-m-N}$. Then $a \in (\mathfrak{P}^N D)^{-1}$, and if the character of $U(K_\mathfrak{P})/U_N(K_\mathfrak{P})$ induced by χ is denoted by the same letter χ, then the Gaussian sum $\tau_a(\chi)$, and the sum $\tau_0(\chi)$, as defined in (5.9), coincide.*

If $K = \mathbb{Q}$, and $\mathfrak{P} = p\mathbb{Z}$, then the same assertion holds for $a = p^{-N}$.

Proof : Put, for shortness, $K_i = K_{\mathfrak{P}_i}$ $(i = 1, 2, \ldots, g)$. Identifying the groups $U(K_\mathfrak{P})/U_N(K_\mathfrak{P})$ and $G(\mathfrak{P}^N)$, and noting that when x runs over a complete set of representatives of $G(\mathfrak{P}^N)$, then cx does the same, we get

$$\tau_0(\chi) = \sum_{x \in G(P^N)} \chi(cx) \exp(2\pi i \lambda(T_{K_1/\mathbb{Q}_p}(cx\pi^{-m-N}))),$$

where λ denotes the function introduced in Sect.5.1.

The elements cx/π^{m+N} are integral in each of the fields $K_2, \ldots, K_g$, thus

$$\exp(2\pi i \lambda(T_{K_i/\mathbb{Q}_p}(cx\pi^{-m-N}))) = 1$$

holds for $i = 2, 3, \ldots g$, and using Corollary 1 to Proposition 6.1 and the equality $\chi(c) = 1$, we arrive at

$$\begin{aligned} \tau_0(\chi) &= \sum_{x \in G(\mathfrak{P}^N)} \chi(cx) \exp(2\pi i \lambda(T_{K/\mathbb{Q}}(cx\pi^{-m-N}))) \\ &= \sum_{x \in G(\mathfrak{P}^N)} \chi(x) \exp(2\pi i \lambda(T_{K/\mathbb{Q}}(ax))). \end{aligned}$$

Our choice of c guarantees that $T_{K/\mathbb{Q}}(ax)$ is a rational number, whose denominator is a power of p, and therefore $\lambda(T_{K/\mathbb{Q}}(ax)) = \{T_{K/\mathbb{Q}}(ax)\}$, where $\{\cdot\}$ denotes the fractional part, and this leads to

$$\tau_0(\chi) = \sum_{x \in G(\mathfrak{P}^N)} \chi(x) \exp(2\pi i T_{K/\mathbb{Q}}(ax)),$$

as asserted.

In the case $K = \mathbb{Q}$ it suffices to observe that the above argument applies with $c = 1$. □

Corollary 1. *Let χ be a primitive character of $G(\mathfrak{P}^N)$ $(N \geq 1)$, and let a be chosen as in Proposition 6.15. Then $|\tau_a(\chi)| = N(\mathfrak{P})^{N/2}$. If $K = \mathbb{Q}$, and $\mathfrak{P} = p\mathbb{Z}$, then $|\tau(\chi)| = p^{n/2}$.*

Proof : This follows from Proposition 5.47 (iii) and the last proposition. □

Corollary 2. *Let* $I = \prod_{i=1}^{r} \mathfrak{P}_i^{N_i}$, *and for* $i = 1, 2, \ldots, r$ *let* a_i *be an element of* K, *satisfying the assumptions of Proposition 6.15. Assume further that* $a \in K$ *satisfies the assumptions of Proposition 6.14 (ii). Then for every primitive character* χ *of* $G(I)$ *we have*

$$|\tau_a(\chi)| = \sqrt{N(I)}.$$

If $K = \mathbb{Q}$, *and* $I = N\mathbb{Z}$, *then* $|\tau(\chi)| = \sqrt{N}$.

Proof : Apply the preceding corollary and Proposition 5.47 (iii). □

6. Now we shall have a closer look at Gaussian sums for primitive real characters in the field of rational numbers. In this case Proposition 6.14 (i) shows that it suffices to deal with $\tau(\chi)$, and the Corollary 2 to Proposition 6.15 and Proposition 6.14 (iii) imply that if χ is real and primitive, then $\tau(\chi)^2 = \chi(-1)M$, where M is the conductor of χ, i.e., $\tau(\chi)$ differs by a fourth root of unity from $\sqrt{M}$. The determination of this root of unity forms the content of the following theorem:

Theorem 6.16. *If* M *is positive and* χ *is a real primitive character of* $G(M)$, *then*

$$\tau(\chi) = \begin{cases} \sqrt{M} & \text{if } \chi \text{ is even.} \\ i\sqrt{M} & \text{if } \chi \text{ is odd.} \end{cases}$$

Proof : The crucial point of the proof lies in the case $M = p$, an odd prime, and we start with the consideration of this case. The group $G(p)$, being cyclic of order $p - 1$, has exactly one subgroup H of index 2, which consists of all squares. If χ is a real primitive character of $G(p)$, then its kernel must equal H, and so we see that $\chi(x)$ is equal to the Legendre symbol. In particular we have $\chi(-1) = (-1)^q$ with $q = (p-1)/2$.

The simple reasoning which now follows is due to Waterhouse [70].

Consider the linear space V of all complex-valued functions defined on $G(p)$. Its dimension equals $p - 1$ and we have two obvious bases in it: one consisting of characteristic functions of element of $G(p)$ i.e., $f_k(x) = \delta_x^k$ $(k = 1, 2, \ldots, p-1)$, and another, consisting of all characters $\{\chi_1, \ldots, \chi_{p-1}\}$ of $G(p)$. Define now a linear map $B : V \longrightarrow V$, defined by

$$B(g)(n) = \sum_{j=1}^{p-1} g(j)\zeta_p^{jn}.$$

Proposition 6.14 (i) implies $B(\chi) = \tau(\chi)\bar{\chi}$ for every character χ of $G(p)$. Since the equality $\chi = \bar{\chi}$ holds only for the two real characters, we see that the matrix of B in the basis $\chi_1, \ldots \chi_{p-1}$ consists of blocks

$$\begin{pmatrix} 0 & \tau(\psi) \\ \tau(\bar{\psi}) & 0 \end{pmatrix}$$

corresponding to pairs ψ, $\bar{\psi}$ of conjugate non-real characters, and of two diagonal entries equal to -1 (which corresponds to the trivial character) and $\tau(\chi)$, χ denoting the unique non-trivial real character. Therefore we have

$$\det B = -\tau(\chi) \prod_{\psi} \left(-\tau(\psi)\tau(\bar{\psi})\right),$$

the product taken over pairs $(\psi, \bar{\psi})$ of conjugate non-real characters. Since Corollary 2 to Proposition 6.15 and Proposition 6.14 (iii) imply the equality $-\tau(\psi)\tau(\bar{\psi}) = -p\psi(-1)$, we obtain

$$\begin{aligned} \det B &= -(-p)^{(p-3)/2}\tau(\chi) \prod_{\psi} \psi(-1) \\ &= (-1)^{(p-1)/2+[(p-1)/4]} p^{(p-3)/2}\tau(\chi), \end{aligned}$$

since there are exactly $[(p-1)/4]$ pairs of conjugated odd characters ψ.

Now we compute the determinant of B, utilizing the basis $f_1, \ldots, f_{p-1}$, and obtain

$$\det B = \det\left(\zeta_p^{kn}\right)_{1 \le k,n \le p-1}.$$

Thus

$$\det B = \zeta_p^{1+2+\ldots+(p-1)} \mathrm{Vand}(\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}),$$

where by

$$\mathrm{Vand}(a_1, \ldots, a_k) = \prod_{i<j} (a_j - a_i)$$

we denote the Vandermonde determinant, corresponding to $a_1, \ldots, a_k$,

Therefore

$$\det B = \prod_{1 \le l < k \le p-1} \left(\zeta_p^k - \zeta_p^l\right),$$

and writing $x = \cos(\pi/p) + i\sin(\pi/p)$ we obtain

$$\det B = \prod_{l<k} x^{k+l}(x^{k-l} - x^{l-k}) = \prod_{l<k} x^{k+l} \prod_{l<k} \left(2i \sin \frac{(k-l)\pi}{p}\right).$$

Because of

$$\sum_{1 \le l < k \le p-1} (k+l) = \frac{p(p-1)(p-2)}{2},$$

the first factor equals $(-1)^{(p-1)/2}$, and second equals a positive quantity multiplied by $i^{(p-1)(p-2)/2}$, and comparing this with the previous expression for B we obtain the assertion of the theorem in the case $M = p$, an odd prime.

The cases $M = 1$ and $M = 2$ are trivial, and for $M = 4$ and 8 the assertion can be directly verified, as for the only non-trivial character of

$G(4)$ the Gaussian sum equals $2i$, and for the two non-trivial real characters of $G(8)$ one easily obtains the values $\sqrt{8}$ and $i\sqrt{8}$ for their Gaussian sums.

Proposition 6.13 shows that real primitive characters of $G(M)$ exist only if $M = 2^a p_1 \cdots p_r$, where $a = 0, 2$ or 3 and $p_1, \ldots, p_r$ are distinct odd primes, so assume that M has this form, and that χ is a real primitive character of $G(M)$. Write $\chi = \prod_{j=0}^{r} \chi_j$, where $\chi_0 = 1$ if $a = 0$ and χ_0 is a primitive real character of $G(2^a)$ otherwise, and for $i = 1, 2, \ldots, r$ one has $\chi_i(x) = \left(\frac{x}{p_i}\right)$. For simplicity put $p_0 = 2^a$. Using the Corollary to Proposition 6.14 we can write

$$\tau(\chi) = \prod_{i=0}^{r} \chi_i(M/p_i)\tau(\chi_i),$$

and using the already proved part of our theorem and the fact that the character χ_i is odd for $i \geq 1$ if and only if $p_i \equiv 3 \pmod 4$, we get

$$\tau(\chi) = i^{s+\epsilon}\sqrt{M} \prod_{i=0}^{r} \chi_i(M/p_i),$$

where s is the number of prime divisors of M congruent to 3 mod 4 and ϵ is 1 if χ_0 is odd and vanishes otherwise. Using the quadratic reciprocity law we obtain now

$$\begin{aligned}
\prod_{i=0}^{r} \chi_i(M/p_i) &= \chi_0(p_1 \cdots p_r) \prod_{i=1}^{r} \left(\frac{p_0 \cdots p_{i-1} p_{i+1} \cdots p_r}{p_i} \right) \\
&= \chi_0(p_1 \cdots p_r) \prod_{i=1}^{r} \prod_{\substack{0 \leq j \leq r \\ j \neq i}} \left(\frac{p_j}{p_i} \right) \\
&= \chi_0(p_1 \cdots p_r) \prod_{j=1}^{r} \left(\frac{p_0}{p_j} \right) \prod_{1 \leq i < k} \left(\frac{p_i}{p_k} \right) \left(\frac{p_k}{p_i} \right) \\
&= \chi_0(p_1 \cdots p_r) \prod_{j=1}^{r} \left(\frac{p_0}{p_j} \right) \prod_{1 \leq i < k} (-1)^{(p_i - 1)(p_k - 1)/4} \\
&= (-1)^{s(s-1)/2} \chi_0(p_1 \cdots p_r) \prod_{j=1}^{r} \left(\frac{p_0}{p_j} \right),
\end{aligned}$$

and the equality

$$\tau(\chi) = (-1)^{s(s-1)/2} i^{s+\epsilon} \sqrt{M} \chi_0(p_1 \cdots p_r) \prod_{j=1}^{r} \left(\frac{p_0}{p_j} \right)$$

follows.

Now we have to consider three cases, namely $p_0 = 1$, $p_0 = 4$ and $p_0 = 8$.

In the first case we have $\epsilon = 0$ and hence

$$\tau(\chi) = \begin{cases} \sqrt{M} & \text{if } 2|s, \\ i\sqrt{M} & \text{if } 2 \nmid s, \end{cases}$$

but $\chi(-1) = (-1)^s$, and we obtain the asserted formula.

In the second case we have $\epsilon = 1$, $\left(\frac{p_0}{p_i}\right) = 1$ for $i \geq 1$ and $\chi_0(p_1 \cdots p_r) = (-1)^s$, because the non-trivial character of $G(4)$ equals $\chi_0(x) = (-1)^{(x-1)/2}$. By putting together these equalities one easily confirms the truth of the theorem in this case.

Finally we are left with $p_0 = 8$. Denote by t_i the number of prime divisors of M congruent to $i \bmod M$ for $i = 1, 3, 5, 7$, and observe that there are two primitive real characters mod 8, one assuming for $x = 3, 5, 7$ the values $1, -1, -1$, and the other assuming the values $-1, -1, 1$. For the first of them we have $\epsilon = 1$, and for the second $\epsilon = 0$.

With this notation we have

$$\prod_{j=1}^{r} \left(\frac{p_0}{p_j}\right) = \prod_{j=1}^{r} (-1)^{(p_j^2-1)/8} = (-1)^{t_3+t_5},$$

and

$$\chi_0(p_1 \cdots p_r) = \begin{cases} (-1)^{t_5+t_7} & \text{if } \epsilon = 1, \\ (-1)^{t_3+t_5} & \text{if } \epsilon = 0. \end{cases}$$

Moreover, $s = t_3 + t_7$ and

$$\chi(-1) = \chi_0(-1) \prod_{i=1}^{r} \chi_i(-1) = \chi_0(-1) \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) = \chi_0(-1)(-1)^s.$$

Now we can easily obtain the assertion of the theorem by checking the resulting cases:

(a) $s \equiv 0, 1 \pmod 4$, $\epsilon = 1$. Here

$$\tau(\chi) = i^{s+1}\sqrt{M}(-1)^{t_5+t_7+t_3+t_5} = (-1)^s i^{s+1}\sqrt{M},$$

and this implies our assertion.

(b) $s \equiv 0, 1 \pmod 4$, $\epsilon = 0$. Here

$$\tau(\chi) = i^s\sqrt{M},$$

in accordance with our assertion.

(c) $s \equiv 2, 3 \pmod 4$, $\epsilon = 1$. Here

$$\tau(\chi) = i^{s+1}\sqrt{M}(-1)^{t_5+t_7+t_3+t_5+1} = (-i)^{s+1}\sqrt{M},$$

again with accordance with the theorem, which can be seen after a short computation.

(d) $s \equiv 2, 3 \pmod 4$, $\epsilon = 0$ in which case

$$\tau(\chi) = i^s\sqrt{M}(-1)^{t_3+t_5+t_3+t_5+1} = -i^s\sqrt{M},$$

which equals $\sqrt{M}$ for $s \equiv 2 \pmod 4$, and equals $i\sqrt{M}$ for $s \equiv 3 \pmod 4$. □

We conclude this subsection with a counterpart to the last theorem:

Theorem 6.17. *Let p be an odd prime, and let χ be a primitive character of $G(p)$. If the quotient $\chi(p)/\sqrt{p}$ is a root of unity, then $\chi(x) = \left(\frac{x}{p}\right)$.*

Proof : Let χ be a non-trivial character of $G(p)$, and denote by $\chi_1(x)$ the real character $\left(\frac{x}{p}\right)$. Assume that with a root of unity ϵ we have $\tau(\chi) = \epsilon\sqrt{p}$. Obviously the number $\tau(\chi)$ lies in the field $K = \mathbb{Q}(\zeta_p, \zeta_{p-1}) = \mathbb{Q}(\zeta_r)$ with $r = p(p-1)$. To get more information about this field observe that the values of χ form a subgroup of the group of all roots of unity of order $p-1$, and so we may write, for $a = 1, 2, \ldots, p-1$, $\chi(a) = \zeta_{p-1}^m$, with $m = m(a)$.

By Theorem 6.16 we have $\tau(\chi_1) = \eta\sqrt{p}$ with $\eta = 1$ or i, depending on the residue of p mod 4. Hence we get

$$\tau(\chi) = \epsilon\eta^{-1}\tau(\chi_1),$$

and since both Gaussian sums occurring here lie in K, we infer that $\epsilon\eta^{-1} \in K$. Now Theorem 4.27 implies the equality

$$\epsilon\eta^{-1} = (\zeta_{p-1}\zeta_p)^k,$$

with a suitable k. For $a = 1, 2, \ldots, p-1$ let g_a be that element of the Galois group of $K/\mathbb{Q}$ which maps ζ_p to ζ_p^a and fixes ζ_{p-1}. We have $g_a(\chi(x)) = \chi(x)$ and $g_a(\tau(\chi)) = \tau_a(\chi)$, and using Proposition 6.14 (i) we obtain

$$\begin{aligned}(\zeta_{p-1}\zeta_p^a)^k &= g_1((\zeta_{p-1}\zeta_p)^k) = g_a(\epsilon\eta^{-1}) = g_a(\tau(\chi))/g(\tau(\chi_1)) \\ &= \tau_a(\chi)/\tau_a(\chi_1) = \overline{\chi(a)\chi_1(a)}\tau(\chi)/\tau_1(\chi) \\ &= \overline{\chi(a)}\chi_1(a)(\zeta_{p-1}\zeta_p)^k,\end{aligned}$$

which implies $\zeta_p^{ak} = \overline{\chi(a)}\chi_1(a)\zeta_p^k$, i.e.,

$$\chi(a) = \zeta_p^{(a-1)k}\left(\frac{a}{p}\right) \in \mathbb{Q}(\zeta_p)$$

$a = 1, \ldots, p-1$, showing that all values of χ lie in $\mathbb{Q}(\zeta_p)$. But $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}$ and we see that χ is a real character, necessarily equal to the symbol of Legendre. □

7. We conclude this section with the proof of the *Kronecker-Weber theorem*:

Theorem 6.18. *If $K/\mathbb{Q}$ is a normal extension with an Abelian Galois group, then K is contained in a suitable cyclotomic field $\mathbb{Q}(\zeta_m)$.*

This result belongs properly to the class-field theory. We have decided to include it here, because one of its proofs, due Shafarevich [51], is a very illuminating example of the application of $\mathfrak{p}$-adic methods to the theory of algebraic numbers.

Proof : Observe first that it suffices to prove the theorem for cyclic extensions of a prime-power degree. Indeed, if $K/\mathbb{Q}$ is Abelian, $Gal(K/\mathbb{Q}) = \prod_{i=1}^{r} C_{p_i^{n_i}}$ is the factorization of its Galois group into cyclic factors of prime-power orders, and for $i = 1, 2, \ldots, r$ we put $G_j = \prod_{i \neq j} C_{p_i^{n_i}}$, then the field L_j corresponding to G_j by Galois theory is a cyclic extension of $\mathbb{Q}$ of degree $p_j^{n_j}$, and the field K is the composite of $L_1, L_2, \ldots, L_r$.

Now fix a prime power q^m, let $S = \{p_1, \ldots, p_r\}$ be a finite set of primes, and denote by $K = K_{q^m,S}$ the composite of all cyclic extensions of the rationals, whose degrees divide q^m and in which only primes from S can ramify, i.e., whose discriminants are divisible only by primes lying in S. It follows from Corollary 5 to Proposition 6.2 that the extension $K/\mathbb{Q}$ is finite, and one sees easily that its Galois group is a subgroup of a suitable power of the group C_{q^m}. The theorem will be established if we show that every field $K_{q^m,S}$ is contained in a cyclotomic field.

For every prime $p \neq q$ denote by $Z = Z_{q^m,p}$ the maximal subfield of $\mathbb{Q}(\zeta_p)$ such that the order of every element of its Galois group is a divisor of q^m. Moreover for $p = q \neq 2$ let $Z = Z_{q^m,q}$ be the unique subfield of degree q^m of $\mathbb{Q}(\zeta_{q^{1+m}})$, and finally put $Z_{2^m,2} = \mathbb{Q}(\zeta_{2^{m+2}})$. If $p \in S$, then obviously $Z_{q^m,p} \subset K_{q^m,S}$, and our aim will now be the proof the following assertion:

Proposition 6.19. *If $S = \{p_1, \ldots, p_r\}$, then the field $K_{q^m,S}$ coincides with the composite $Z'_{q^m,S}$ of the fields $Z_{q^m,p_1}, \ldots, Z_{q^m,p_r}$.*

Note that the theorem is an immediate consequence of this proposition, since the fields Z_{q^m,p_i} are by definition contained in cyclotomic fields, and so is their composite.

Proof : Since in the extension $Z_{q^m,p}/\mathbb{Q}$ only the prime p ramifies, the Corollary to Theorem 4.26 leads us to the equality

$$\left[Z'_{q^m,S} : \mathbb{Q}\right] = \prod_{i=1}^{r} \left[Z_{q^m,p_i} : \mathbb{Q}\right].$$

Since $Z_{q^m,p_i} \subset \mathbb{Q}(\zeta_{p_i}^{m+2})$ we see that $p_i\mathbb{Z}$ becomes in Z_{q^m,p_i} a power of a prime ideal of degree 1 by Theorem 4.40 and Proposition 4.3. This shows that the

degree of $Z_{q^m,p_i}/\mathbb{Q}$ equals the ramification index e_i of this extension, and we obtain $[Z'_{q^m,S} : \mathbb{Q}] = e_1 \cdots e_r$, showing that in view of $Z_{q^m,S} \subset K_{q^m,S}$ it suffices to establish the inequality $[K_{q^m,S} : \mathbb{Q}] \leq e_1 \cdots e_r$.

Assume for a moment that the following lemma is true:

Lemma 6.20. *If $L = L_{q^m,p}$ is the composite of all cyclic extensions of $\mathbb{Q}_p$ whose degrees divides q^m, then L coincides with the composite of $Z_{q^m,p}$ and the unique unramified extension $W_{q^m,p}$ of degree q^m of the field $\mathbb{Q}_p$.*

We deduce now our proposition from this lemma, and then provide a proof of it. It is clear that for $p \in S$ we have $K_{q^m,S} \subset L_{q^m,p}$ and so the lemma implies $K_{q^m,S} \subset Z_{q^m,p}W_{q^m,p}$. Since $W_{q^m,p}/\mathbb{Q}_p$ is unramified, and the ramification index over $\mathbb{Q}_p$ of the closure of $Z_{q^m,p}$ in L equals e_i, we obtain that the ramification index of p_i in $K_{q^m,S}/\mathbb{Q}$ cannot exceed e_i, due to Theorem 5.11 (iv) and the multiplicativity of ramification indices.

The monodromy theorem (Corollary 2 to Proposition 6.8) implies that the Galois group of $K_{q^m,S}$ is generated by its inertia subgroups, and, as it is Abelian, its order cannot exceed the product of orders of these subgroups, which does not exceed $e_1e_2 \cdots e_r$. We pointed out already that this implies Proposition 6.19.

Thus everything has been reduced to the proof of Lemma 6.20, which we will now give:

Proof of Lemma 6.20: Fix the primes p, q and the exponent m, and write, for shortness, $L = L_{q^m,p}$, $W = W_{q^m,p}$ and $Z = Z_{q^m,p}$.

The inclusion $WZ \subset L$ is obvious, and hence it suffices to establish the equality of degrees of $WZ/\mathbb{Q}_p$ and $L/\mathbb{Q}_p$.

Consider first the case $p \neq q$. The Galois group G of $L/\mathbb{Q}_p$ is a subgroup of some power of the group C_{q^m}, and therefore its cyclic subgroups are of the form C_q^a with $a = 0, 1, \ldots, m$. This shows that W is the maximal unramified subfield of L, since by Corollary 2 to Theorem 5.25 unramified extensions are cyclic, and the degree of $W/\mathbb{Q}_p$ equals q^m. Thus L/W is fully and tamely ramified of degree $e(L/\mathbb{Q}_p)$, since $p \nmid q$. Corollary 2 to Theorem 5.34 shows that the extension L/W is cyclic and its first ramification group G_1 is trivial. However its Galois group is a subgroup of G and so we get

$$e(L/\mathbb{Q}_p) = [L : W] | q^m. \tag{6.3}$$

Let R be the ring of integers of W, S the ring of integers of L, and let $S = R[\pi]$ with π generating the prime ideal of S. Its existence is assured by Theorem 5.27. Moreover let σ be a generator of the inertia group of $L/\mathbb{Q}_p$, which actually coincides with $Gal(L/W)$, and let $\tau \in G$ induce the map $x \longrightarrow x^p$ in the residue class field. The existence of τ is assured by Proposition 5.33. Observe that $\pi^2 \nmid \sigma(\pi)$. Indeed, otherwise we would have $\sigma(\pi) = c\pi^2$ with $c \in S$, hence

$$\sigma^{-1}(c)\sigma^{-1}(\pi)^2 = \sigma^{-1}(c\pi^2) = \pi,$$

and, in view of $\pi|\sigma^{-1}(\pi)$, we would get $\pi^2|\pi$, which is absurd.

Therefore we may write

$$\sigma(\pi) \equiv a\pi \pmod{\pi^2}$$

with a certain $a \in U(S)$, and similarly

$$\tau(\pi) \equiv b\pi \pmod{\pi^2},$$

with $b \in S$.

Since $L/\mathbb{Q}_p$ is Abelian we have

$$\begin{aligned} a^p\tau(\pi) &\equiv \tau(a\pi) \equiv \tau(\sigma(\pi)) \equiv \sigma(\tau(\pi)) \\ &\equiv \sigma(b)a\pi \equiv ba\pi \equiv a\tau(\pi) \pmod{\pi^2}, \end{aligned}$$

hence

$$a^{p-1}\tau(\pi) \equiv \tau(\pi) \pmod{\pi^2},$$

and $a^{p-1} \equiv 1 \pmod{\pi}$.

Now note that for $k = 1, 2, \ldots$ we have

$$\sigma^k(\pi) \equiv a^k\pi \pmod{\pi^2},$$

hence $\sigma^{p-1}(\pi) \equiv \pi \pmod{\pi^2}$, showing that $\sigma^{p-1} \in G_1 = \{id_L\}$, thus

$$e(L/\mathbb{Q}_p) = e(L/W) = [L : W] | p - 1, \tag{6.4}$$

and from (6.3) and (6.4) we get $e(L/\mathbb{Q}_p)|(p-1, q^m)$.

Since the polynomial $(X^p - 1)/(X - 1)$ is irreducible over $\mathbb{Q}_p$, the equality $[Z\mathbb{Q}_p : \mathbb{Q}_p] = (p - 1, q^m)$ follows, and in view of $Z\mathbb{Q}_p \cap W = \mathbb{Q}_p$ (because $Z\mathbb{Q}_p$ is fully ramified, and W is unramified) we obtain

$$[ZW : \mathbb{Q}_p] = f(L/\mathbb{Q}_p)(p - 1, q^m) \geq f(L/\mathbb{Q}_p)e(L/\mathbb{Q}_p) = [L : \mathbb{Q}_p],$$

and thus $L = ZW$, as asserted.

Now consider the case $p = q \neq 2$. Here the Galois group of the extension $ZW/\mathbb{Q}_p$ equals $C_{p^m}^2$, and we have to show that the Galois group G of $L/\mathbb{Q}_p$ has at most two independent generators. To do this it is sufficient to prove that the Galois group of $L_{p,p}/\mathbb{Q}_p$ has at most two generators. Indeed, assume that this is true and let r be the number of independent generators of G. Then there exist subfields $L_1, \ldots, L_r$ of L, distinct from $\mathbb{Q}_p$, which are independent in the following sense: for each $i = 1, 2, \ldots, r$ the intersection of L_i with the composite of the remaining fields L_j equals $\mathbb{Q}_p$. But selecting in every field L_i a subfield of degree p over $\mathbb{Q}_p$ we obtain r independent subfields of $L_{p,p}$, and one sees easily that this implies $r \leq 2$.

Hence we have to establish the inequality $[L_{p,p} : \mathbb{Q}_p] \leq p^2$. We first need a simple lemma:

Lemma 6.21. *Let $M = \mathbb{Q}_p(\zeta_p)$, let σ be a generator of $Gal(M/\mathbb{Q}_p)$ and let a be an element of M which is not a p-th power in M. Moreover, define k by $\sigma(\zeta_p) = \zeta_p^k$. Then the extension $M(a^{1/p})/\mathbb{Q}_p$ is Abelian if and only if there exists $c \in M$ with $\sigma(a) = a^k c^p$.*

Proof : Put $L = M(a^{1/p})$. Assume first that $L/\mathbb{Q}_p$ is Abelian, and lift σ to an automorphism of this extension. If $b = \sigma(a)$, then $b^{1/p} \in L$, and so we can choose a generator g of the cyclic group $Gal(L/M)$ such that $g(a^{1/p}) = \zeta_p a^{1/p}$ and $g(b^{1/p}) = \zeta_p^r b^{1/p}$ holds with a certain r. This shows that the element $a^{r/p} b^{-1/p}$ is invariant under g, hence lies in M, i.e., with a suitable $c \in M$ we have $b^{1/p} = c a^{r/p}$, and $b = a^r c^p$. Now define two automorphisms, g_1 and g_2 of $L/\mathbb{Q}_p$, assuming $g_1(a^{1/p}) = \zeta_p a^{1/p}$ and $g_{1|_M} = id_M$, whereas $g_{2|_M} = \sigma$ and $g_2(a^{1/p}) = b^{1/p} = c a^{r/p}$. Then

$$c\zeta_p^r a^{r/p} = g_1(c a^{r/p}) = g_1 g_2(a^{1/p}) = \ g_2 g_1(a^{1/p}) = g_2(\zeta_p a^{1/p}) = \zeta_p^k c a^{r/p},$$

which leads us to $k = r$ and proves the "only if" part of the lemma. Conversely, if $\sigma(a) = a^k c^p$ with $c \in M$, then $M(a^{1/p})$ is normal and, repeating our argument in the reversed order we obtain the abelianity of the considered extension. □

Let now $K/\mathbb{Q}_p$ be a cyclic extension of degree p, and put $M = \mathbb{Q}_p(\zeta_p)$. Fix a generator σ of $Gal(M/\mathbb{Q}_p)$, and define k by $\sigma(\zeta_p) = \zeta_p^k$. Note that k is a primitive root mod p.

The extension KM/M is cyclic, and we can write $KM = M(a^{1/p})$ with a certain $a \in M$. The extension $KM/\mathbb{Q}_p$ is the composite of two Abelian extensions, hence is Abelian itself, and the preceding lemma shows that it is determined by an element of $V = H/(M^*)^p$, where H is the multiplicative group of non-zero elements $a \in M$, for which $\sigma(a) = a^k c^p$ holds with $c \in M$.

One can regard V as a linear space over $\mathbb{F}_p$, and if $L_1, \ldots, L_j$ are cyclic extensions of $\mathbb{Q}_p$, independent in the sense defined above, then the corresponding elements of V are linearly independent. Indeed, otherwise, if we would write $L_i M = M(a_i^{1/p})$ $(i = 1, 2, \ldots, j)$, then the images $x_1, \ldots, x_j$ of the a_i's in V would, after renumbering, satisfy $x_1 = \sum_{i=2}^{j} n_i x_i$ with $n_2, \ldots, n_j \in \mathbb{F}_p$, and this would imply $a_1 = b^p \prod_{i=2}^{j} a_j^{n_j}$, hence $ML_1 \subset ML_2 \cdots L_j$. But the independence of the L_i's gives $[L_1 \cdots L_j : \mathbb{Q}_p] = p^j$, and $[L_2 \cdots L_j : \mathbb{Q}_p] = p^{j-1}$, thus $[ML_1 \cdots L_j : \mathbb{Q}_p] = p^j(p-1)$ and $[ML_2 \cdots L_j : \mathbb{Q}_p] = p^{j-1}(p-1)$, showing that ML_1 cannot be contained in $ML_2 \cdots L_j$.

Put $\pi = 1 - \zeta_p$. One sees easily that π is a generator of the prime ideal $\mathfrak{P}$ of M. Observe now that every class of V has a representative in $U_1(M)$. Indeed, if ν denotes the exponent of M, and $a = a_1 \pi^t \in H$, with $a_1 \in U(M)$, $t = \nu(a)$ and $\sigma(a) = a^k c^p$ $(c \in M)$ holds, then

$$kt + p\nu(c) = \nu(\sigma(a)) = \nu(a) = t,$$

thus $p|(k-1)t$. Since p does not divide $k-1$, it has to divide t, whence $a^{1/p}$ and $a_1^{1/p}$ determine the same extension of M, and so lie in the same coset of $H \bmod (M^*)^p$, showing that every class of V has a representative in $U(M)$. Since $U(M) \sim U(M)/U_1(M) \times U_1(M)$, and the order of the first factor is not divisible by p, hence every its element is a p-th power, we find that in every class of (M^*) there is a principal unit, as asserted.

Now we show that $U_1(M)^p = U_{1+p}(M)$. Since $e(M/\mathbb{Q}_p) = p-1$, Lemma 5.19 implies $U_{1+p}(M) \subset U_2(M)^p \subset U_1(M)^p$, and so it remains to show that every p-th power of a principal unit lies in $U_{1+p}(M)$. To obtain this, let $u \in U_1(M)$ and write $u = 1 + a\pi + b\pi^2$, with $0 \leq a \leq p-1$ and b being an integer of M. Now

$$u^p = (1 + a\pi + b\pi^2)^p = \sum_{i+j+l=p} \frac{p!}{i!j!l!} a^j b^l \pi^{j+2l},$$

and one observes that the only terms of this expansion which are not divisible by π^{1+p} are 1, $pa\pi$ and $a^p\pi^p$. Therefore

$$u^p \equiv 1 + pa\pi + a^p\pi^p \pmod{\mathfrak{P}^{1+p}}.$$

But we may write $p = \epsilon\pi^{p-1}$, where

$$\epsilon = \prod_{l=1}^{p-1} \left(1 + \zeta_p + \cdots + \zeta_p^{l-1}\right)$$

is a unit, and since by our choice of π we have $\zeta_p \equiv 1 \pmod{\mathfrak{P}}$, we infer that

$$\epsilon \equiv (p-1)! \equiv -1 \pmod{\mathfrak{P}},$$

by Wilson's theorem. This establishes $\pi^{1+p}|pa\pi + a^p\pi^p$, hence $u^p \in U_{1+p}(M)$.

Let H_1 be the group of residue classes $a \bmod \pi^{1+p}$ for which $a \in U_1(M)$ and $\sigma(a) \equiv a^k \pmod{\mathfrak{P}^{1+p}}$. The last result implies that $\#V \leq \#H_1$. Now observe that $A = 1 + \pi^p \in H_1$. Indeed, we have $A^k \equiv 1 + k\pi^p \pmod{\mathfrak{P}^{1+p}}$, and, on the other hand,

$$\sigma(A) = 1 + (1 - \zeta_p^k)^p = 1 + \pi^p(1 + \zeta_p + \cdots + \zeta_p^{k-1})^p \equiv 1 + k\pi^p \pmod{\mathfrak{P}^{1+p}},$$

thus $A \in H_1$. Moreover we have $\zeta_p \in H_1$ and therefore it remains to show that A and ζ_p generate H_1, since then we would have $\#V \leq \#H_1 \leq p^2$.

First let $a \in H_1 \cap U_2$ $(a \neq 1)$, so that we have $a \equiv 1 + a_1\pi^i \pmod{\mathfrak{P}^{1+i}}$ with a rational integer a_1 not divisible by p and $2 \leq i \leq p$. Then

$$\sigma(a) \equiv 1 + a_1\sigma(\pi^i) \equiv 1 + a_1 k^i \pi^i \pmod{\mathfrak{P}^{1+i}},$$

but we have also

$$\sigma(a) \equiv a^k \equiv 1 + a_1 k\pi^i \pmod{\mathfrak{P}^{1+i}},$$

showing that $k^{i-1} \equiv 1 \pmod{\mathfrak{P}}$. Hence we get $i = p$, because k is a primitive root mod p. This establishes the inclusion $H_1 \cap U_2 \subset H_1 \cap U_p$. Moreover, for $a \in H_1 \setminus U_2$ write $a \equiv 1 + b\pi \pmod{\mathfrak{P}^2}$ with $b \in \mathbb{Z}$, and observe that $a\zeta_p^b \in U_2 \cap H_1$, hence every element $a \in H_1$ satisfies

$$a \equiv \zeta_p^b(1 + c\pi^p) \pmod{\mathfrak{P}^{1+p}}$$

with some integral c. In view of $A^c = (1 + \pi^p)^c \equiv 1 + c\pi^p \pmod{\mathfrak{P}^{1+p}}$, we obtain $a \equiv \zeta_p^b A^c \pmod{\mathfrak{P}^{1+p}}$, and thus indeed H_1 is generated by ζ_p and A. As already observed, this settles the case under consideration.

In the last case we have $p = q = 2$. In this case the extension $\mathbb{Q}_2 Z/\mathbb{Q}_2$ has the group $C_2 \times C_{2^m}$ for its Galois group, and so the composite WZ has its Galois group over $\mathbb{Q}_2$ equal to $C_2 \times C_{2^m} \times C_{2^m}$. To obtain the equality $WZ = L$ we have to show that the Galois group of $L/\mathbb{Q}_2$ has three generators, at least one of which is of order 2. As in the preceding case, the first assertion reduces to $m = 1$, and so we have to prove that $Gal(L_{2,2}/\mathbb{Q}_2)$ has three generators. But we know already that $\mathbb{Q}_2$ has seven quadratic extensions, generated by the square roots of -1, 2, 5, -10, -5, -2, and 10, and one sees immediately that the first three fields form a maximal independent system. This proves that the Galois group of $L_{2,2}/\mathbb{Q}_2$ has 3 generators.

Finally, if $Gal(L_{2^m,2}/\mathbb{Q}_2)$ would have all generators of orders at least equal to 4, then $Gal(L_{4,2})$ would be isomorphic to C_4^3, and so every quadratic extension of $\mathbb{Q}_2$ would be contained in a cyclic quartic extension. But this fails for the field $Q(\sqrt{-1})$. Indeed, write $i = \sqrt{-1}$ and assume that $\mathbb{Q}_2(i)$ is contained in a field $K = \mathbb{Q}_2(i, \sqrt{a + bi})$ whose Galois group over $\mathbb{Q}_2$ equals C_4. Since K is normal, it is generated over $\mathbb{Q}_2(i)$ also by $\sqrt{a - bi}$, and so with suitable $A, B \in \mathbb{Q}_2$ we must have

$$a - bi = (a + bi)(A + Bi)^2.$$

Observe that by putting

$$\begin{aligned} \sigma(\sqrt{a + bi}) &= \sqrt{a - bi} = \sqrt{a + bi}(A + Bi), \\ \sigma(i) &= i, \end{aligned}$$

we define an automorphism of $K/\mathbb{Q}_2$ of order 4, hence generating the Galois group of $K/\mathbb{Q}_2$. Since σ^2 is the only non-trivial element of the Galois group of $K/\mathbb{Q}_2(i)$ it takes $\sqrt{a + bi}$ into $-\sqrt{a + bi}$ and we get

$$\begin{aligned} -\sqrt{a + bi} &= \sigma^2(\sqrt{a + bi}) = \sigma(\sqrt{a + bi}(A - Bi)) \\ &= (A^2 + B^2)\sqrt{a + bi}, \end{aligned}$$

thus $A^2 + B^2 = -1$. However this is impossible in $\mathbb{Q}_2$, and this contradiction achieves the proof of the lemma. □

We pointed out already that the theorem is a consequence of the lemma just proved. □

6.2. Adeles and Ideles

1. In this section K will be an algebraic number field, and Ω the set of all its non-equivalent non-trivial valuations, Archimedean and non-Archimedean. We shall assume that all valuations are normalized, i.e., for non-Archimedean v we have $v(x) = N(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$, if v corresponds to a prime ideal $\mathfrak{p}$ of R_K with exponent $\nu_\mathfrak{p}$, and if v is Archimedean, and corresponds to the embedding F of K into the complex field, then

$$v(x) = \begin{cases} |F(x)| & \text{if } F(K) \text{ is real,} \\ |F(x)|^2 & \text{otherwise.} \end{cases}$$

It is convenient to arrange the embeddings $F_1, F_2, \ldots$ of K in $\mathbb{C}$ (considering only one from each pair of conjugated complex embeddings) so that the first $r_1(K)$ of them are real, and the remaining are complex. Later we shall use this arrangement without further comment.

For any $v \in \Omega$ denote by K_v the completion of K under v, and let R_v be the ring of integers of K_v in the case of non-Archimedean v. In the Archimedean case we put $R_v = K_v$. The restricted direct product[1] of the additive groups K_v^+ with respect to the subgroups R_v^+ is called the *adele group* of K, and its elements are called *adeles* of K. Incidentally, this group has also a ring structure induced by multiplication in the factors. The resulting ring is called the *adele ring* of K, and will be denoted by A_K. Since the multiplication is obviously continuous, we conclude by Lemma 1 of Appendix I that A_K is a locally compact topological ring. For any finite subset $S \subset \Omega$ denote by A_S the group $\prod_{v\in S} K_v^+ \times \prod_{v\notin S} R_v^+$. From the definition of the restricted product it follows that the topology induced in A_S by the topology in A_K coincides with the product topology, and every group A_S is open in A_K. Obviously the union of all groups A_S exhausts the full adele group.

The invertible elements of A_K are called *ideles*. They form a group I_K, the *idele group* of K. However, it is not convenient to give that group the topology inherited from A_K, and we shall endow it with another restricted product topology. To do this observe that in the multiplicative group K_v^* we can select for all non-Archimedean v's the subgroup $U(K_v)$ of units, which is compact and open, and it can be immediately seen that if we define additionally $U(K_v) = K_v^*$ for Archimedean v's, then the restricted product of the groups K_v^* with respect to $U(K_v)$ equals I_K. Only this topology on the idele group will be used in the sequel. If for a finite set $S \subset \Omega$ we put

$$I_S = \prod_{v\in S} K_v^* \times \prod_{v\notin S} U(K_v),$$

then, as in the case of adeles, we obtain that the group I_S inherits the product topology from I_K, and is open in I_K. One choice of the set S is of

[1] For the definition and properties of restricted direct products see Appendix I.

particular importance: $S = S_\infty$, the set of all Archimedean valuations of K. In this case we denote I_S by U_K and call its elements *unit ideles*.

Observe that for every $x \in K$ we have $x \in R_v$ for almost all (i.e., for all except finitely many) v, and for every non-zero $x \in K$ we have $x \in U(K_v)$ for almost all v. This allows us to define a canonical embedding i of K in A_K and of K^* in I_K by means of $i(x) = \langle x_v \rangle_v$, where we put $x_v = x$ for non-Archimedean v, and $x_v = F_i(x)$, if v is Archimedean and corresponds to the embedding F_i. Put $i(K) = A_0 \subset A_K$, $i(K^*) = I_0 \subset I_K$, and call these images the *ring of principal adeles* and the *group of principal ideles*, respectively. In sequel we shall often identify an element $a \in K$ with its image $i(a)$ in A_K, or I_K.

Note that a non-zero principal adele is an idele.

For any idele $x = \langle x_v \rangle$ define its volume $V(x)$ by

$$V(x) = \prod_{v \in \Omega} v(x_v).$$

This infinite product is convergent, since for every x it contains only finitely many terms distinct from 1, and so this definition makes sense. Theorem 3.5 implies that the volume of a principal idele equals 1, hence I_0 lies in the kernel J_K of the map V of I_K into the multiplicative group of positive reals. This simple fact implies the following observation:

Proposition 6.22. *(i) The ring A_0 is a discrete subring of A_K.*

(ii) The group I_0 is a discrete subgroup of I_K.

Proof : (i) It suffices to find a neighbourhood of zero in A_K, not containing non-zero principal adeles. Let us take for that neighbourhood the set

$$O = \{\langle a_v \rangle : \ v(a_v) < 1 \ (v \in S_\infty), \ v(a_v) \leq 1 \ (v \notin S_\infty)\}.$$

If a non-zero principal adele $i(a)$ lies in O, then it is an idele with $V(i(a)) < 1$, which is possible only for $a = 0$.

(ii) Let U be the neighbourhood of unity in I_K, consisting of all ideles $\langle a_v \rangle$ which for Archimedean v satisfy $v(a_v < 1)$, and lie in the open subgroup U_K. Now observe that a principal idele lies in U_K if and only if it is a unit of K. Thus if an idele $i(a)$ lies in U, then a is a unit of K and $a - 1 \in R_K$. However

$$|N_{K/\mathbb{Q}}(a-1)| = \prod_{v \in S_\infty} v(a_v - 1) < 1,$$

which is possible only for $a = 1$. □

The factor group A_K^+ / A_0^+ is called the *adele class group*, and similarly the group $C(K) = I_K / I_0$ is called the *idele class group*.

Proposition 6.23. *The adele class group is compact, whereas the idele class group is not compact.*

Proof : Let $\alpha = \langle a_v \rangle$ be an arbitrary adele. We shall prove the existence of a compact set $B \subset A_K^+$, independent of α, and such that in the coset $\alpha \bmod A_0^+$ there is an adele from B. First choose a rational integer m so that for all v we have $ma_v \in R_v$, and denote by P the set of all prime ideals of R_K dividing $m\mathbb{Z}$. Put $N = \max_{\mathfrak{p} \in P} \nu_{\mathfrak{p}}(m)$, and let $x \in R_K$ be a solution of the system

$$x \equiv ma_{v_{\mathfrak{p}}} \pmod{\mathfrak{p}^N} \quad (\mathfrak{p} \in P)$$

of congruences. For $b_v = a_v - x/m$ we have, for every $v \notin S_\infty$ the inequality

$$v(b_v) = v(ma_v - x)/v(m) \leq 1,$$

and so the adele $\langle b_v \rangle$, which lies in the same coset as α, has all its coordinates in R_v. If $S_\infty = \{v_1, \ldots, v_s\}$, then since the set

$$\{[F_1(t), \ldots, F_s(t)] : \ t \in R_K\}$$

forms an s-dimensional lattice in the Euclidean s-space, we can select a suitable $t_0 \in R_K$ so that the point $[b_{v_1} - F_1(t_0), \ldots, b_{v_s} - F_s(t_0)]$ lies in a compact set, independent of α. This implies $v_i(b_{v_i} - F_i(t_0)) < C$ $(i = 1, 2, \ldots, s)$ for a certain $C > 0$, thus the adele $\langle b_v - i(t_0) \rangle$ lies in a compact set independent of α, and is in the same class as α. This establishes the first assertion, and to prove the second it suffices to observe that the volume $V(x)$ is an unbounded and continuous function on the idele class-group, and so this group cannot be compact. □

2. Let $G(K)$ be the group of all fractional ideals of K in which we consider the discrete topology. There is a canonical homomorphism of I_K onto this group. To define it consider an arbitrary idele $\alpha = \langle a_v \rangle$ and put

$$f(\alpha) = \prod_{v \notin S_\infty} \mathfrak{p}_v^{\nu_v(a_v)},$$

where ν_v is the exponent corresponding to the prime ideal $\mathfrak{p}_v$. Obviously $f : \ I_K \longrightarrow G(K)$ is a continuous surjective homomorphism with kernel U_K, thus $I_K/U_K \sim G(K)$.

Proposition 6.24. *The group $H(K)$ of ideal classes in K is isomorphic to the quotient group $I_K/U_K I_0$.*

Proof : Consider the homomorphism $g : \ G(K) \longrightarrow H(K)$, mapping every ideal to the class to which it belongs. Then $g \circ f$ maps I_K onto $H(K)$ and its kernel equals

$$\{x : \ f(x) \text{ is principal}\} = \{x : \ f(x) \in f(I_0)\} = \{x : \ x \in I_0 \cdot \mathrm{Ker} f\} = I_0 U_K.$$

□

Corollary. *Every open subgroup of $C(K)$ is of finite index.*

Proof : Let G be an open subgroup of $C(K)$, and let H be that subgroup of I_K which is mapped on G be the canonical map. Obviously H is open, and so contains a neighbourhood of unity of the form

$$\{\langle x_v\rangle : \ v(x_v - 1) < \epsilon \text{ for } v \in S_\infty, x_v \in U(K_v) \text{ for } v \notin S_\infty\},$$

and also the subgroup generated by it, which turns out to be U_K, since it has a non-void interior. So it suffices to show that the image of U_K has a finite index in $C(K)$, but this follows from the proposition and the finiteness of the class-number. □

Now we prove a result of importance in the class-field theory:

Theorem 6.25. *The group J_K/I_0 is compact.*

Proof : We shall use the finiteness of the class-group $H(K)$, as well as Dirichlet's theorem on the structure of the unit group $U(K)$. Let $I_1, \ldots, I_h$ be ideals of R_K, representing all ideal classes of $H(K)$. Now let $\alpha = \langle a_v\rangle \in J_K$ be given, and let $I = f(\alpha)$ be the corresponding ideal, which can be written as $I = cI_j$ with $c \in K^*$ and suitable $1 \leq j \leq h$. Observe that there exist ideles $\beta_1, \ldots, \beta_h$ in J_K, satisfying $f(\beta_i) = I_i$ for $i = 1, 2, \ldots, h$. Indeed, the equation $f(\beta) = I_i$ restricts only the non-Archimedean coordinates of β, and we can adjust the Archimedean coordinates to obtain $V(\beta) = 1$. Since $f(\alpha\beta_j^{-1}/c) = 1$, we see that the idele $\alpha\beta_j^{-1}/c$ lies in $J_K \cap U_K$.

Now let $S_\infty = \{v_1, \ldots, v_{r+1}\}$ with r being the unit rank of K, and define a homomorphism $L : \ U_K \cap J_K \longrightarrow \mathbb{R}^r$ by means of

$$L(\langle u_v\rangle) = [\log v_1(u_{v_1}), \ldots, \log v_r(u_{v_r})].$$

This map is surjective since, given $[t_1, \ldots, t_r] \in \mathbb{R}^r$, there exist $u_1, \ldots, u_r$ with $v_i(u_i) = \exp(t_i)$ for $i = 1, 2, \ldots, r$, and then, assuming $v_{r+1}(u_{v_{r+1}}) = \exp(-(t_1 + \cdots + t_r))$, and putting $u_v = 1$ for $v \notin S_\infty$, we get an idele $u = \langle u_v\rangle \in J_K \cap U_K$ with $L(u) = [t_1, \ldots, t_r]$.

The proof of Theorem 3.13 shows that the images $L(\epsilon_i)$ of the fundamental units $\epsilon_1, \ldots, \epsilon_r$ of K are linearly independent, and thus span the full space $\mathbb{R}^r$. Denote by P the set of all ideles in $J_K \cap U_K$ whose images in $\mathbb{R}^r$ can be written in the form $\sum_{i=1}^r x_i L(\epsilon_i)$ with $0 \leq x_i \leq 1$ $(i = 1, 2, \ldots, r)$. This set is obviously compact, and, moreover, for every idele $u \in J_K \cap U_K$ there is a unit ϵ of K such that ϵu lies in P. Applying this observation to $u = \alpha\beta_j^{-1}/c$ we obtain $\alpha = \epsilon c \beta_j \alpha_1$ with $\alpha_1 \in P$, and thus every idele from J_K has an idele from $\mathcal{X} = \bigcup_{i=1}^h \beta_i P$ in its class mod I_0. Since $\mathcal{X}$ is a fixed compact set, the compactness of J_K/I_0 follows. □

Corollary. *If $D(K)$ is the connected component of the unit element of $C(K)$, then the factor group $C(K)/D(K)$ is compact and totally disconnected.*

Proof : The second assertion is trivial, and to prove the first it suffices to show that every coset of $C(K)$ mod $D(K)$ contains an element of $J_K.I_0$. Take any idele $\xi = \langle x_v \rangle$, and let t be its volume. Since the group of ideles $\langle a_v \rangle$ with $a_v = 1$ for non-Archimedean v is connected, the class determined by the idele $\eta = \langle y_v \rangle$, with $V(\eta) = t$ and $y_v = 1$ for $v \notin S_\infty$ lies in $D(K)$. Hence the classes determined by ξ and $\xi\eta^{-1}$ are in the same coset, but is is clear that $\xi\eta^{-1}$ determines a class in J_K/I_0. □

3. The general theory of restricted direct products (see Appendix I) gives a way of constructing a standard Haar measure in the groups of adeles and ideles once the Haar measures in K_v^+ and K_v^* have been fixed. Recall that in the case of non-Archimedean v we have chosen that Haar measure μ_v on K_v^+ which gives to the ring R_v the measure $N(D_v)^{-1/2}$, where D_v denotes the different of $K_v/\mathbb{Q}_p$, p being the characteristic of the residue class field of K_v. On the multiplicative group we choose the measure μ_v^* defined by

$$\mu_v^*(A) = \frac{N(P)}{N(P)-1} \int_A \frac{d\mu(x_v)}{v(x)},$$

$P = P_v$ being the prime ideal of R_v. This measure gives to the group of units of R_v the measure $N(D_v)^{-1/2}$. In the case of $v \in S_\infty$ we proceed as follows: if $K_v = \mathbb{R}$, then μ_v is the usual Lebesgue measure and

$$\mu_v^*(A) = \int_A \frac{d\mu_v(x)}{|x_v|}.$$

If $K_v = \mathbb{C}$, then μ_v will be the double of the Lebesgue plane measure, and

$$\mu_v^*(A) = \int_A \frac{d\mu_v(x)}{|x_v|^2}.$$

Note that all measures μ_v are self-dual, provided that in the Archimedean case we make the slightly artificial identification between K_v^+ and its dual, shown in Appendix I.

The resulting Haar measures in A_K and I_K will be denoted by m_A and m_I, respectively. Note that the first of them is self-dual. Observe also that for every idele α we have the equality $dm_A(\alpha x) = V(\alpha)dm_A(x)$, resulting from the corresponding result for the measures μ_v, which in turn is easily established through Corollary 2 to Lemma 5.43.

Our next aim is to prove the strong approximation theorem, but first we need an auxiliary result:

Proposition 6.26. *There exists a positive constant C such that if $\alpha = \langle a_v \rangle$ is an idele with $V(\alpha) \geq C$, then there exists a principal idele $\beta = \langle b_v \rangle$ such that for all v one has $v(b_v) \leq v(a_v)$.*

Proof : We need a lemma from the theory of topological groups:

Lemma 6.27. *Let G be a locally compact Abelian group and H its countable discrete subgroup such that G/H is compact. If A is an open subset of G with a sufficiently large Haar measure, then there exist $x_1, x_2 \in A$, lying in the same coset with respect to H.*

Proof : Let U be a neighbourhood of the unit element of G, which satisfies $U \cap H = \{e\}$ and has finite measure. By the compactness of G/H there exist $x_1, \ldots, x_s \in G$ such that if $\varphi : G \longrightarrow G/H$ denotes the canonical map and $V = \bigcup_{i=1}^{s} x_i U$, then $G/H = \varphi(V)$. Let B be the measure of V, and let A be an open subset of G, all elements of which lie in distinct cosets. Then the set $A_1 = \varphi^{-1}(\varphi(A)) \cap V$ is open, because φ is open and continuous, and its measure does not exceed B. Every element of A_1 can be uniquely put in the form ah with $a \in A$, $h \in H$. Write $X_h = \{a \in A : ah \in A_1\}$. These sets are all open in view of $X_h = A_1 h^{-1} \cap A$, and we have $A = \bigcup_h X_h$, $A_1 = \bigcup_h hX_h$, both sums being disjoint. This gives the equality of measures of A and A_1, and so the measure of A does not exceed a fixed constant. □

Now consider the set

$$X = \{\langle x_v \rangle \in A_K : \ v(x_v) < v(a_v)/2 \ (v \in S_\infty), v(x_v) \leq v(a_v) \ (v \notin S_\infty)\},$$

which is open in A_K. Let us compute its measure. Let S be the set consisting of all Archimedean valuations of K, all non-Archimedean v's with $v(a_v) > 1$, and all non-Archimedean v's such that $K_v/\mathbb{Q}_p$ is ramified. Then $X \subset A_S$ and the definition of our measure gives

$$m_A(X) = \prod_{v \in S} \int_{X_v} d\mu_v(x),$$

where X_v is the projection of X on K_v. If v is real, then X_v is of measure $v(a_v)$, and if v is complex, then the measure of X_v equals $\pi v(a_v)$. For non-Archimedean v this measure equals $v(a_v)N(D_v)^{-1/2}$. Thus finally we obtain by Propositions 4.14 and 6.2 the equality

$$m_A(X) = \pi^{r_2} V(\alpha) |d(K)|^{-1/2}.$$

In view of Propositions 6.22 (i) and 6.23 we may now apply Lemma 6.27 and find that if the volume $V(\alpha)$ is large enough, then there exist two distinct adeles in X , whose difference is a principal adele, say $\beta = \langle b_v \rangle$. But obviously this adele satisfies $v(b_v) \leq v(a_v)$ for all v's, and since β is non-zero, it is an idele. □

The last proposition allows us to prove the *strong approximation theorem*:

Theorem 6.28. *If $v_0 \in \Omega$, then for every finite set $\Omega_1 \subset \Omega$ not containing v_0, every system $a_v \in K_v$ $(v \in \Omega_1)$, and every $\epsilon > 0$ there exists a principal adele $\beta = \langle b_v \rangle$ such that $v(b_v - a_v) < \epsilon$ for $v \in \Omega_1$ and $v(b_v) \leq 1$ for $v \notin \Omega_1$, $v \neq v_0$.*

Proof : Proposition 6,23 gives the existence of a compact set $A \subset A_K^+$, such that every class of adeles has its representative in A. Obviously it must be contained in a set of the shape $\{\langle x_v \rangle : \ v(x_v) \leq \eta_v\}$ with suitable $\eta_v > 0$, almost all of which are equal to 1. Apply Proposition 6.26 to $\gamma = \langle \gamma_v \rangle$ with $0 < v(\gamma_v) < \epsilon/\eta_v$ for $v \in \Omega_1$, $0 < v(\gamma_v) \leq 1/\eta_v$ for $v \notin \Omega_1$, $v \neq v_0$ and $v_0(\gamma_{v_0})$ sufficiently large. This gives the existence of a principal idele $\langle d_v \rangle$ with

$$v(d_v) \leq \begin{cases} \epsilon/\eta_v & \text{if } v \in \Omega_1, \\ 1/\eta_v & \text{if } v \notin \Omega_1, v \neq v_0. \end{cases}$$

Now put $a_v = 0$ for $v \notin \Omega_1$ and write

$$\langle a_v d_v^{-1} \rangle = \langle b_v \rangle + \langle c_v \rangle,$$

with $\langle b_v \rangle \in A$ and principal $\langle c_v \rangle$. Then

$$v(a_v - c_v d_v) = v(b_v d_v)$$

and it follows easily that the adele $\langle c_v d_v \rangle$ satisfies our assertion. □

4. Now we present the proof of a theorem of Hecke concerning the discriminant $d(L/K)$. To do this we have to introduce, following Fröhlich [60b], a new kind of discriminant of a finite extension of an algebraic number field based on the discriminants $\partial(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ defined in Chap. 5 for the extension of $\mathfrak{p}$-adic fields. First we prove a simple lemma:

Lemma 6.29. *The factor-group I_K/U_K^2 is algebraically isomorphic with the subgroup of the product $\prod_v K_v^*/U(K_v)^2$, consisting of all elements $\langle x_v \rangle$ satisfying $x_v \in U(K_v)/U^2(K_v)$ for almost all v's.*

Proof : The embedding of the idele group I_K into the product of all groups K_v^* obviously induces such an isomorphism. □

Now let K be an algebraic number field, let L/K be its finite extension, and denote by $\Omega(K)$, $\Omega(L)$ the sets of inequivalent normalized valuations of K and L, respectively. We shall define the discriminant $\partial(L/K)$, which will be an element of the factor group I_K/U_K^2. Let v be a normalized valuation of K, and let $w_1, \ldots, w_m$ form the full system of non-equivalent normalized valuations of L, whose restrictions to K are equivalent to v. For simplicity we shall in this situation say later, rather not precisely, that the w_i's are extensions of v. Theorem 3.3 shows that if v ranges over $\Omega(K)$, then we obtain in this way all valuations of $\Omega(L)$. Put

$$\partial(L/K) = \langle \partial_v(L/K) \rangle \in \prod_v K_v^*/U(K_v)^2,$$

where the components $\partial_v(L/K)$ are defined as follows:

If $K_v = \mathbb{C}$, then put $\partial_v(L/K) = 1$, and if $K_v = \mathbb{R}$ and t is the number of complex fields L_{w_i} $(i = 1, 2, \ldots, m)$, then put $\partial_v(L/K) = (-1)^t$. For non-Archimedean v put

$$\partial_v(L/K) = \prod_{i=1}^{m} \partial(L_{w_i}/K_v).$$

Proposition 5.14 (ii) shows that for almost all v the component $\partial_v(L/K)$ lies in $U(K_v)/U(K_v)^2$, and so by Lemma 6.29 we can regard the discriminant $\partial(L/K)$ as an element of I_K/U_K^2, Its main properties are given in the following proposition:

Proposition 6.30. *(i) If*

$$g: \ I_K/U_K^2 \longrightarrow I_K/U_K = G(K)$$

is the homomorphism induced by the embedding of $U_K^2 \subset U_K$, *then* $g(\partial(L/K))$ *equals* $d(L/K)$, *the usual discriminant of the extension* L/K.

(ii) The extension L/K *is unramified if and only if* $\partial(L/K) \in U_K/U_K^2$.

(iii) If $K \subset L \subset M$, *then*

$$\partial(M/K) = \partial(L/K)^{[M:L]} N_{L/K}(\partial(M/L)), \tag{6.5}$$

where $N_{L/K}: \ I_L/U_L^2 \longrightarrow I_K/U_K^2$ *is the map induced by the norm maps* $\prod_w N_{L_w/K_v}$ *(where* w *ranges over all extensions of* v *to* L*) at all components* v.

Proof: The assertion (i) results from Proposition 5.14 (i) and the observation that the value of g does not depend on the Archimedean components, and (ii) follows immediately from (i) and the discriminant theorem (Corollary 3 to Theorem 4.24).

The assertion (iii) for non-Archimedean components is a consequence of Proposition 5.14 (iii), and to obtain the same for Archimedean components we have to examine them more careful. If K_v is complex, then there is nothing to prove, since the v-components of both sides of (6.5) are equal 1. Assume thus that v is real and let $w_1, \ldots, w_r$ be the real, and $w_{r+1}, \ldots, w_m$ the complex extensions of v to L. By Theorem 3.3 they are all determined by embeddings of L into the complex field, which map K onto a fixed subfield K_0 of the reals, and are all equal on K_0. This shows that $r + 2(m - r) = [L : K]$. Similarly, every real valuation w_i has, say, a_i real and b_i complex extensions to M with $a_i + 2b_i = [M : L]$, and every complex w_i has $[M : L]$ complex extensions to M and, of course, no real ones. This shows that v has $b = b_1 + \cdots + b_r + (m - r)[M : L]$ complex extensions to M, and so

the v-component on the left-hand side of (6.5) equals $(-1)^b$. Now look at the right-hand side. The v-component of $\partial(L/K)^{[M:L]}$ equals $(-1)^{(m-r)[M:L]}$, and for $i = 1, 2, \ldots, r$ the w_i-component of $\partial(M/L)$ equals $(-1)^{b_i}$, whereas for the remaining w_i's it equals 1. This shows that the v-component of the norm is $(-1)^{b_1+\cdots+b_r}$ (because the extension L_{w_i}/K_v for real w_i is trivial), and for complex w_i it equals 1. Finally, we see that the v-components of both sides of (6.5) are equal. □

Now we can prove Hecke's theorem:

Theorem 6.31. *If L/K is a finite extension of an algebraic number field K, then the class of its discriminant $d(L/K)$ in the class-group $H(K)$ is a square.*

Proof : We prove first that $\partial(L/K)$ lies in $I_K^2 I_0/U_K$. The easiest method of doing it requires some simple facts about algebras which we shall now indicate. Let M be a field, let N_i/M be for $i = 1, 2, \ldots, r$ finite separable extensions of M, contained in a fixed algebraic closure of M, and put

$$E = \bigoplus_{i=1}^{r} N_i.$$

Choose for $i = 1, 2, \ldots, r$ an M-basis A_i of N_i, and form from them an M-basis for A. One defines its discriminant $d(A)$ as the product of the discriminants $d_{N_i/M}(A_i)$ (as defined in Chap. 2). Note that if we start with other M-bases $B_1, \ldots, B_r$ of $N_1, \ldots, N_r$ and put $B = \bigcup_i B_i$, then by Proposition 2.9 (ii) the discriminants $d(A)$ and $d(B)$ will differ by a factor, which is a square in M.

Now we apply this setup to our situation. Proposition 6.1 shows that for every non-Archimedean $v \in \Omega(K)$ we have an isomorphism

$$L \otimes_K K_v \sim \bigoplus_{i=1}^{m} L_{w_i},$$

where $w_1, \ldots, w_m$ are all inequivalent extensions of v to L. In each field L_{w_i} choose a K_v-basis consisting of elements of L, which can be done since L spans L_{w_i} over K_v, and put them together to obtain a K_v-basis $a_1, \ldots, a_n$ of $L \otimes_K K_v$. Since the a_i's lie in L we obtain that their discriminant D is an element of K. Now let $\langle D_v \rangle$ be an idele of K, representing $\partial(L/K)$. For non-Archimedean v we may write

$$D_v = \prod_{i=1}^{m} D'_{w_i},$$

where D'_{w_i} is a representative of $\partial(L_{w_i}/K_v)$. If we choose in each field L_{w_i} a K_v-basis with discriminant D'_{w_i} and put them together, we obtain a basis of

$L \otimes_K K_v$ which has D_v for its discriminant. This implies $D_v/D \in (K_v^*)^2$, at least for all non-Archimedean v. Since for complex v we have $K_v^* = (K_v^*)^2$, it remains to show that for real v the quotient D_v/D is positive, but we have $D_v = (-1)^s$, where s is the number of complex extensions of v to L, and the argument used in the proof of Proposition 2.15 shows that the sign of D also equals $(-1)^s$.

Thus we got the inclusion $\partial(L/K) \in I_K^2 I_0/U_K^2$, hence every representative of $\partial(L/K)$ is mapped by the canonical map $I_K \longrightarrow I_K/I_0U_K \sim H(K)$ into a square, and Proposition 6.30 (i) shows now that $d(L/K)$ lies in a class which is a square. □

The discriminant $\partial(L/K)$ introduced in this subsection gives more information about the extension L/K than the usual discriminant $d(L/K)$, which is an ideal. In fact $\partial(L/K)$ seems to be the true generalization of the numerical discriminant $d(K)$ for relative extensions. It has been shown by Fröhlich [60b,d] that it is possible to describe the structure of R_L as an R_K-module in terms of $\partial(L/K)$, and in particular one can obtain necessary and sufficient conditions for the existence of a relative integral basis. This approach works also for arbitrary Dedekind domains (Fröhlich [61]). We shall present his result in Chap. 7, after proving certain auxiliary results, necessitating the use of analytical tools (see Corollary 1 to Theorem 7.42).

5. We conclude this section with the proof of the functional equation for the zeta-functions of I_K, which we shall define below after introducing certain results on characters and quasicharacters of the groups of adeles and ideles.

We know already that A_K^+ is self-dual because all groups K_v^+ are such, but in the argument which follows an explicit form of this self-duality is needed:

Proposition 6.32. *Let*

$$\chi_v(t_v) = \begin{cases} \exp\left(2\pi i \lambda_p(T_{K_v/Q_p}(t_v))\right), & \text{if } v \notin S_\infty, \\ \exp(-2\pi i t_v) & \text{if } v \text{ is real,} \\ \exp(-4\pi i \mathrm{Re}\ (t_v)) & \text{if } v \text{ is complex,} \end{cases}$$

where λ_p is the function occurring in the canonical form of a character of $\mathbb{Q}_p$. Then $\mathbf{X}(\langle t_v \rangle) = \prod_v \chi_v(t_v)$ is a character of A_K^+, and every character of A_K^+ is of the form $X_\alpha(t) = \mathbf{X}(\alpha t)$, with $\alpha \in A_K^+$.

Proof : Clear. □

Corollary. *(i) The map $\alpha \mapsto \chi_\alpha$ is an isomorphism between A_K^+ and its dual.*

(ii) For any two adeles α, β one has $\chi(\alpha\beta(t)) = \chi_a(\beta t)$.

(iii) One has $X_a(t) = 1$ for all $t \in A_0$ if and only if $a \in A_0$.

Proof : The assertions (i) and (ii) are direct consequences of the proposition. To prove (iii) let $H = \{a \in A_K^+ : \ X_a(A_0) = 1\}$, and observe that for $t \in K$ the expression

$$-T_{K/\mathbb{Q}}(t) + \sum_{v \notin S_\infty} \lambda_p(T_{K_v/\mathbb{Q}_p}(t_v) = -T_{K/\mathbb{Q}}(t) + \sum_p \lambda_p(T_{K/\mathbb{Q}}(t)$$

is a rational integer. This shows that if $a, t \in A_0$, then $X_a(t) = 1$, i.e. $A_0 \subset H$. Proposition 6.23 shows that the group A_K^+/A_0 is compact, hence its dual group is discrete, and therefore H, as a subgroup of the latter, is also discrete, and it follows that the quotient group H/A_0 is discrete. However, we have

$$H/A_0 \subset \hat{A_K^+}/A_0 \sim A_K^+/A_0,$$

thus H/A_0 is compact, and therefore finite. It remains to observe that H is a linear space over the infinite field A_0, and this implies $A_0 = H$. □

Let us recall that any continuous homomorphism of I_K into the multiplicative group of the complex field is called a *quasicharacter* of I_K (see Appendix I). We shall be mostly interested in quasicharacters of I_K which are trivial on I_0. The following proposition describes them:

Proposition 6.33. *(i) If q is a quasicharacter of I_K trivial on J_K, then $q(x) = V(x)^s$ with a suitable complex s, and conversely, for every complex s, $V(x)^s$ is a quasicharacter of I_K trivial on J_K. Such quasicharacter q is a character if and only if* Re $s = 0$, *in which case we have $q(x) = V(x)^{it}$ for some real t.*

(ii) If q is a quasicharacter of I_K trivial on I_0, then $q(x) = \chi(x)V(x)^s$, where s is a complex number, and χ is a character of I_K trivial on I_0. Conversely, every pair $[\chi, s]$ determines a quasicharacter $\chi(x)V(x)^s$ of I_K trivial on I_0. Two pairs $[\chi, s]$, $[\chi_1, s_1]$ determine the same quasicharacter if and only if Re $s =$ Re s_1, *and we have $\chi_1(x) = \chi(x)V(x)^{it}$ with $t =$* Im $(s - s_1)$. *In particular one can always select a real s.*

Proof : (i) If q is a quasicharacter of I_K trivial on J_K, then q depends only on $V(x)$, and so we must have $q(x) = f(V(x))$, where f is a quasicharacter of the multiplicative group of positive reals, thus $f(t) = t^s$ with a suitable complex s, hence $q(x) = V(x)^s$. The remaining parts of (i) become clear if one remembers that for Re $s \neq 0$ the function $V(x)^s$ is unbounded.

(ii) Theorem 6.25 shows that J_K/I_0 is compact, hence for every quasicharacter q of I_K trivial on I_0 its restriction to J_K is in fact a character. Denote it by χ, and since J_K is a closed subgroup of I_K, we can extend χ to a character of I_K. If χ_1 and χ_2 are two such extensions, then $\chi_1\chi_2^{-1}$ is trivial on J_K, and so by (i) we must have $\chi_1(x)\chi_2^{-1}(x) = V(x)^{it}$ with a real t, thus

$$\chi_2(x) = \chi_1(x)V(x)^{it} \tag{6.6}$$

Moreover $q\chi_1^{-1}$ is trivial on J_K and again by (i) we infer that $q(x) = \chi_1(x)V(x)^s$. Equality (6.6) shows that the character χ_1 is determined up to the factor $V(x)^{it}$. The remaining assertions are now evident. □

The number Re s, which, by the last proposition, is uniquely determined by a quasicharacter q of I_K trivial on I_0, is called the *exponent* of q and will be denoted by $\exp q$.

Let Q_0 be the group of all quasicharacters of I_K which are trivial on I_0, and let AnJ_K denote the annihilator of J_K in Q_0, i.e., the subgroup of Q_0 formed by all quasicharacters trivial on J_K. The next lemma permits to make a convenient choice of the set of representatives of the cosets of Q_0 mod AnJ_K:

Lemma 6.34. *In every coset of* Q_0 mod AnJ_K *there is a unique character* χ *of* I_K *such that for* $x = \langle x_v \rangle$ *we have*

$$\chi(x) = \prod_v \chi_v(x_v),$$

where χ_v *is a character of* K_v^*, *which for almost all* v *is trivial on* $U(K_v)$, *and for* v *Archimedean has the form*

$$\chi_v(x_v) = \left(\frac{x_v}{|x_v|}\right)^{m_v} v(x_v)^{it_v},$$

with real t_v, $\sum_{v \in S_\infty} t_v = 0$, *and*

$$m_v \in \begin{cases} \mathbb{Z} & \text{if } v \text{ is complex,} \\ \{0,1\} & \text{if } v \text{ is real.} \end{cases}$$

Proof : The form of the character χ results from the description of characters of I_K given in Theorem VIII of Appendix I. Moreover, Proposition 6.33 shows that every coset of Q_0 mod AnJ_K contains characters, and characters lying in the same coset differ by a factor of the form $V(x)^{it}$ with real t. For every $\chi \in Q_0$ consider $T(\chi) = \sum_{v \in S_\infty} t_v$. For the character $\chi'(x) = \chi(x)V(x)^{it}$ (with $t \in \mathbb{R}$) we get $T(\chi') = T(\chi) + t(r_1(K) + r_2(K))$, hence there is exactly one value of t giving $T(\chi') = 0$, and clearly χ and χ' lie in the same coset mod AnJ_K. □

Characters satisfying the conditions of this lemma are called *normalized characters*.

Let $\{\chi_a\}$ be the set of all characters obtained according to the last lemma, and denote by Q_a the coset mod AnJ_K determined by χ_a. Every quasicharacter from this coset can be written in a unique way in the form

$$q(x) = \chi_a(x)V(x)^s, \tag{6.7}$$

with a suitable $s \in \mathbb{C}$. In this way the elements of the coset Q_a can be described with the use of a complex parameter s, and the group Q_0 can be treated as a family of $\#(Q_0/AnJ_K)$ copies of the complex plane.

There is another way of describing the normalized characters χ_a which we shall now present. Let J'_K be the subgroup of J_K consisting of all ideles $\langle a_v \rangle$ with $a_v = 1$ for non-Archimedean v's, and whose Archimedean components are of the form $a_v = t^{\epsilon_v/s}$, where $s = r_1(K) + r_2(K)$, t is positive and independent of v and

$$\epsilon_v = \begin{cases} 1 & \text{if } v \text{ is real,} \\ 1/2 & \text{if } v \text{ is complex.} \end{cases}$$

One sees that the group J'_K is topologically isomorphic with the multiplicative group of positive reals with the usual topology, the isomorphism being given by

$$t \mapsto \langle t^{1/s}, \ldots, t^{1/2s}, \ldots, 1, 1, \ldots \rangle.$$

Moreover we have the topological isomorphism $I_K \sim J_K \times J'_K$, and so it is possible to choose in J_K a Haar measure $\mu_J(x)$ having the property that the Haar measure m_I on I_K equals the product of μ_J and the standard Haar measure

$$\mu(A) = \int_A \frac{dt}{t},$$

on the multiplicative group of positive reals transferred to J'_K, dt being the differential of the usual Lebesgue measure on $\mathbb{R}^+$.

Proposition 6.35. *A character χ of I_K is normalized if and only if it is trivial on J'_K.*

Proof : If $\chi = \prod_v \chi_v$ is normalized, then for Archimedean v we have

$$\chi_v(x_v) = \left(\frac{x_v}{|x_v|}\right)^{m_v} v(x_v)^{it_v},$$

with $\sum t_v = 0$. If $x = \langle x_v \rangle = \langle t^{1/s}, \ldots \rangle \in J'_K$ (resp. $x = \langle t^{1/2s}, \ldots \rangle$, if $r_1 = 0$), then $\chi(x) = t^{iA}$ with $A = \sum t_v/s = 0$, and thus χ trivializes on J'_K.

Conversely, if χ is trivial on J'_K, then for every $t > 0$ we must have

$$\frac{\log t}{s} \sum t_v = 2\pi N_t,$$

with a certain $N_t \in \mathbb{Z}$, which shows that the ratio $N_t/\log t$ does not depend on t, which can happen only if $N_t = 0$, and thus the sum $\sum t_v$ vanishes. $\square$

Now let f be a complex-valued function defined on I_K about which we assume that for all quasicharacters $q \in Q_0$ with $\exp q > 1$ the *Mellin transform*

$$\tilde{f}(q) = \int_{I_K} f(x)q(x)dm_I(x)$$

is well-defined. If we now fix a coset Q_a, and consider only the quasicharacters which lie in it, then we can, by (6.7), consider $\tilde{f}$ as a function of the complex variable s, defined in the open half-plane Re $s > l = 1$. To stress this fact we shall write $\tilde{f}(q) = Z(f, s, \chi_a)$, or, if the coset Q_a is fixed, $\tilde{f}(q) = Z(f, s)$, and call $\tilde{f}$ the *zeta-function* associated with f. The zeta-functions so defined are meromorphic and satisfy a functional equation, provided f satisfies certain regularity assumptions. This result forms the main part of the next theorem:

Theorem 6.36. *Let f be a complex-valued function defined on A_K, and satisfying the following conditions:*

(a) Both f and its Fourier transform $\hat{f}$ are continuous and integrable,

(b) The two series

$$\sum_{t \in A_0} f(a(x+t)) \quad \text{and} \quad \sum_{t \in A_0} \hat{f}(a(x+t))$$

are uniformly convergent for (a, x) lying in an arbitrary, but fixed, compact subset of the product $I_K \times A_K$,

(c) If g, g_0 are the restrictions of f, respectively $\hat{f}$ to I_K, then for every $t > 1$ the functions $g(x)V(x)^t$ and $g_0(x)V(x)^t$ are integrable in I_K.

Then the following holds:

(i) For every fixed coset Q_a of Q_0 mod *AnJ_K the integral*

$$Z(g, s) = \int_{I_K} g(x)q(x)dm_I(x)$$

with q as in (6.7)*, represents a regular function of s in the open half-plane* Re $s > 1$. *This function can be continued to a meromorphic function.*

(ii) If $Q_a = AnJ_K$ is the zero coset, i.e., $\chi_a(x) = 1$, then $Z(g, s, 1)$ can have at most two single poles at $s = 0$ and $s = 1$, and its residues there are equal to $-h\kappa f(0)$ and $h\kappa\hat{f}(0)$, respectively, with $h = h(K)$ being the class-number of K, and

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2}R(K)}{w(K)\sqrt{|d(K)|}}, \tag{6.8}$$

where r_1, r_2 have their usual meaning, $R(K)$ is the regulator of K, $d(K)$ is its discriminant and $w(K)$ is the number of roots of unity lying in K.

(iii) If Q_a is not the zero coset, then $Z(g, s, \chi_a)$ has a continuation to an entire function.

(iv) (The functional equation) *If $\chi_{a^{-1}}$ lies in the coset inverse to Q_a, then for all $s \in \mathbb{C}$ we have*

$$Z(g, s, \chi_a) = Z(g_0, 1 - s, \chi_{a^{-1}}). \tag{6.9}$$

(v) For all $c_1 < c_2$ and $\epsilon > 0$ the function $Z(g, s, \chi_a)$ is bounded in $\{s : c_1 \leq \operatorname{Re} s \leq c_2, |s| > \epsilon, |s-1| > \epsilon\}$. For non-principal χ_a this applies to every strip $c_1 \leq \operatorname{Re} s \leq c_2$.

Proof: (i) Assumption (c) implies the existence of the integral defining $Z(g, s)$ for every s in the half-line $\operatorname{Re} s > 1$ because of $|g(x)q(x)| = |g(x)|V(x)^{\exp q}$. Denote by A_1 and A_2 the sets of adeles with $V(x) \geq 1$ and $V(x) \leq 1$, respectively, and for $i = 1, 2$ put

$$B_i = \int_{A_i} g(x)q(x)dm_I(x).$$

Since $J_K = A_1 \cap A_2$ is of measure zero, we have $Z(g, s) = B_1 + B_2$. Observe that for $\sigma = \operatorname{Re} s > 1$ the integrals B_1 and B_2 are both regular functions of s. Indeed, under this assumption we have for $i = 1, 2$ the equality

$$\begin{aligned}
&\frac{1}{\delta}\Big(\int_{A_i} g(x)\chi_a(x)V(x)^{s+\delta}dm_I(x) - \int_{A_i} g(x)\chi_a(x)V(x)^s dm_I(x)\Big) \\
&= \int_{A_i} \frac{1}{\delta} g(x)\chi_a(x)V(x)^s(V(x)^\delta - 1)dm_I(x),
\end{aligned}$$

and since for sufficiently small $\delta > 0$ the integrand is

$$O\left(|g(x)|V(x)^\sigma |\log V(x)|\right),$$

we find, using (c), that B_i is differentiable for $\sigma > 1$. The same argument establishes the differentiability of B_1 in the remaining part of the plane, thus B_1 is entire, and to establish (i) it remains to show that B_2 can be continued to a meromorphic function.

Applying Proposition 6.35 we can write

$$\begin{aligned}
B_2 &= \int_0^1 \frac{dt}{t}\left(\int_{J_K} g(tj)q(tj)d\mu_J(j)\right) \\
&= \int_0^1 \frac{dt}{t}\left(\int_{J_K} g(tj)\chi_a(j)t^s d\mu_J(j)\right) = \int_0^1 t^{s-1}\int_{J_K} g(tj)\chi_a(j)d\mu_J(j)dt.
\end{aligned}$$

To evaluate the inner integral in the last term of the above equality a preliminary construction is necessary.

In Theorem 6.25 we obtained the existence of a compact set $B \subset J_K$ containing representatives from every class of $J(K)/I_0$. This set has the form

$$B = \bigcup_{i=1}^{h} b_i P,$$

where $b_1, \ldots, b_h$ are ideles with $V(b_i) = 1$, whose images in $I_K/U_K I_0 \sim H(K)$ represent all ideal classes, and P was the set of all ideles from $J_K \cap U_K$ whose images in $\mathbb{R}^r$ through the map

$$L: \ \langle u_v \rangle \mapsto [\log v(u_v)]_{v \in S_\infty, v \neq v'},$$

(where v' is a fixed valuation in S_∞) are of the form

$$\sum_{j=1}^{r} x_j L(\epsilon_j), \quad (0 \leq x_j < 1), \tag{6.10}$$

where the ϵ_j's are fundamental units of K.

Note that if P' is the set of all ideles from $J_K \cap U_K$ whose images under L have the form (6.10), then the set

$$B' = \bigcup_{i=1}^{h} b_i P'$$

represents all classes of $J(K)/I_0$. This set is no longer compact, and, moreover, it may contain several members of the same class of $C(K)$. Let us find under what circumstances this happens. Assume thus that $a_1, a_2 \in b_i P'$ represent the same class of $C(K)$. (Note that elements from distinct summands $b_i P'$ and $b_j P'$ cannot lie in the same class of $C(K)$, since they induce ideals lying in different classes of $H(K)$.) Write $a_1 = b_i p_1$, $a_2 = b_i p_2$ with $p_1, p_2 \in P'$ and principal $p_1 p_2^{-1}$. But

$$L(p_1 p_2^{-1}) = \sum_{j=1}^{r} x_j L(\epsilon_j),$$

where $-1 < x_j < 1$, and since $p_1 p_2^{-1}$ is principal and induces the unit ideal, it must be a unit. Therefore the x_j's are rational integers, and we see that they must vanish, i.e. $L(p_1 p_2^{-1}) = 0$. Hence for every valuation v with one exception we have $v(p_1 p_2^{-1}) = 1$, and the product formula shows that the same must be true also for the excepted valuation. Hence by Theorems 3.3 and 2.5 (i) we see that $p_1 p_2^{-1}$ must be a root of unity, and so finally we get $a_1 = \zeta_w^m a_2$, with $w = w(K)$ and a suitable m. Conversely, if two ideles from P' differ by a factor which is a root of unity, then they lie in the same class of $C(K)$.

In the definition of the mapping L one of the Archimedean valuations was not used. It is convenient to have it complex if there exist complex valuations of K at all, and we shall make this choice whenever possible. Let v' be that valuation. Let us now define

$$P_1 = \{\langle x_v \rangle \in P' : \ 0 \leq \arg x_{v'} < \frac{2\pi}{w}\}$$

which definition in the case of real v' reduces to

$$P_1 = \{\langle x_v \rangle \in P' : \ x_{v'} > 0\}.$$

The foregoing argument shows that the set

$$E = \bigcup_{i=1}^{h} b_i P_1$$

contains exactly one element from every class of $J_K/I_0 \subset C(K)$. Now we compute the measure of E.

Lemma 6.37. *The measure $\mu_J(E)$ of the set E equals $h\kappa$, where κ is defined by (6.8).*

Proof : From the definition of E we readily obtain

$$\mu_J(E) = \sum_{i=1}^{h} \mu_J(b_i P_1) = h\mu_J(P_1),$$

and in addition $\mu_J(P_1) = \mu_J(P')/w$, hence we have to find the measure of P'. An idele $x = \langle x_v \rangle$ lies in P' if and only if it is satisfies the following conditions:

$$v(x_v) = 1 \quad for \quad v \notin S_\infty, \quad V(x) = 1,$$

and

$$0 \leq \sum_{\substack{v \in S_\infty \\ v \neq v'}} A_{v,j} \log v(x_v) < 1 \quad (j = 1, 2, \ldots, r),$$

where v' is a fixed valuation and $[A_{v,j}]$ is the matrix inverse to the matrix whose j-th column equals $L(\epsilon_j)$. Let now Λ be the Cartesian product of P' and the interval $[1, e]$, considering the latter as a subset of J'_K. Thus $\Lambda \subset I_K$, and any pair (a, t) with $a \in P'$, $1 \leq t \leq e$ can be identified with the product at', t' being the idele $[t^{1/s}, \ldots]$. Since the interval $[1, e]$ is of unit measure in J'_K we get $\mu_j(P') = m_I(\Lambda)$. To find $m_I(\Lambda)$ observe that if $S \subset \Omega$ contains all Archimedean valuations, and also all non-Archimedean valuations corresponding to prime ideals ramified in $K/\mathbb{Q}$, then $\Lambda \subset I_S$ and so

$$\mu_J(P') = \int_\Lambda d\mu_S(x),$$

the measure $d\mu_S(x)$ being defined in subsect. 7 of Appendix I.

The idele $u = \langle u_v \rangle$ lies in Λ if and only if $v(u_v) = 1$ holds for $v \notin S_\infty$, $1 \leq V(u) \leq e$ and if we put

$$t_v = \begin{cases} V(u)^{\epsilon_v/s} & \text{if } v \in S_\infty, \\ 1 & \text{otherwise,} \end{cases}$$

then for $j = 1, 2, \ldots, r$ one has

$$0 \leq \sum_{\substack{v \in S_\infty \\ v \neq v'}} A_{v,j} \log v(u_v/t_v) < 1 \quad (j = 1, 2, \ldots, r). \tag{6.11}$$

Moreover, by the definition of the measure μ_S we see that $\mu_J(P')$ equals the product of two integrals: one taken over $\prod_{v \in S \setminus S_\infty} U(K_v)$, and the other taken over the projection Λ_A of Λ into $\prod_{v \in S_\infty} K_v^*$, the integrand being in both cases equal to 1. The first of these integrals equals the product of $N(D_{K_v/\mathbb{Q}_p})^{-1/2}$ taken over all v's at which $K/\mathbb{Q}$ is ramified, hence it equals $|d(K)|^{-1/2}$, and so we are left with the second integral, which we shall call I. Put $s = r_1 + r_2$. If $v_1, \ldots, v_{r_1}$ and $v_{r_1+1}, \ldots, v_s$ are the real, respectively the complex valuations of K, then the integral I is equal to the integral in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of the function

$$\Phi(u_1, \ldots, u_s) = \prod_{i=1}^{s} v_i(u_i)^{-1}$$

taken over the set of all s-tuples

$$(u_1, \ldots, u_s) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

satisfying $\prod_{i=1}^{s} v_i(u_i) = t$, as well as

$$0 \leq \sum_{\substack{1 \leq i \leq r \\ v_i \neq v'}} A_{v_i,j} \log v_i(u_i/t_{v_i}) < 1 \quad (j = 1, 2, \ldots, r)$$

with a certain t in the interval $[1, e]$. If now $X \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the set of all r-tuples $(u_1, \ldots, u_r)$ satisfying $\prod_{i=1}^{r} v_i(u_i) = t$ and $1 \leq v_i(u_i/t_{v_i}) < e$ for certain $1 \leq t < e$ and $v_i \neq v'$, then one sees that

$$I = R(K) \int_X \Phi(u_1, \ldots, u_r) du_1 \cdots du_r.$$

To deal with the last integral we make the following change of variables:

$$\begin{aligned} u_i' &= u_i \quad \text{for} \quad v_i \neq v' \\ u &= u_{v'} \prod_{\substack{1 \leq i \leq r \\ v_i \neq v'}} u_i^{-1}, \end{aligned}$$

which leads to

$$I = \int_1^e \left(\prod_{\substack{1 \leq i \leq r \\ v_i \neq v_0}} \int_{B_{v_i,t}} \frac{du_i'}{v_i(u_i')} \right) \frac{du}{u},$$

where

$$B_{v,t} = \{x \in K_v : \ t^{1/s} \leq v(x) < et^{1/s}\},$$

and one arrives at $I = 2^{r_1}(2\pi)^{r_2}$. Finally we obtain

$$j(E) = \frac{h}{w} \frac{R(K) 2^{r_1} (2\pi)^{r_2}}{\sqrt{|d(K)|}} = h\kappa,$$

as asserted. □

Now we return to the integral B_2, which, as we have seen, equals

$$\int_0^1 t^{s-1} \int_{J_K} g(tj)\chi_a(j) d\mu_J(j) dt, \tag{6.12}$$

and using the fact that every element of J_K can be in exactly one way written as bj with $b \in I_0$ and $j \in E$, we can put the inner integral in the form

$$\begin{aligned} \int_E \sum_{b \in I_0} g(btj)\chi_a(j) d\mu_J(j) &= \int_E \chi_a(j) \sum_{b \in I_0} g(btj) d\mu_J(j) \\ &= \int_E \chi_a(j) \left(\sum_{b \in A_0} f(btj) - f(0) \right) d\mu_J(j). \end{aligned}$$

To evaluate the last integral we need a lemma:

Lemma 6.38. *If the function f satisfies the assumptions of the theorem, then for every idele x we have*

$$\sum_{b \in A_0} f(bx) = \frac{1}{V(x)} \sum_{b \in A_0} \hat{f}(b/x).$$

Proof : We want to apply Poisson's formula (see Appendix I) for the adele group and its subgroup of principal adeles, and to do that we have to check the assumptions. We need a fundamental set $\mathfrak{D}$ of unit measure. From the proof of Proposition 6.23 we infer that if $\omega_1, \ldots, \omega_n$ is an integral basis of $K/\mathbb{Q}$ and $\omega_1', \ldots, \omega_n'$ are the projections of the principal adeles generated by the ω_i's into the product $\prod_{v \in S_\infty} K_v^+$, then for $\mathfrak{D}$ we can take the set of all adeles $\alpha = \langle a_v \rangle$ such that for non-Archimedean v's one has $v(a_v) \leq 1$, whereas the projection of α onto $\prod_{v \in S_\infty} K_v^+$ lies in the set

$$\left\{ \sum_{i=1}^n x_i \omega_i' : \ 0 \leq x_i < 1 \right\}.$$

Using Corollary 1 to Lemma 5.43 and the definition of the discriminant we see that the measure of $\mathfrak{D}$ in fact equals 1. If we define the Haar measure in the adele class-group via the one-to-one map between $\mathfrak{D}$ and A_K^+/A_0, then all assumptions of the Poisson formula are satisfied and we may apply it to the function $f_1(t) = f(xt)$.

First we compute its Fourier transform, so let $\mathbf{X}$ be the character of A_K^+ occurring in Proposition 6.32, and put $X_a(t) = \mathbf{X}(at)$ for $a \in A_K$. Then, using Proposition 6.32 and its Corollary we get

$$\begin{aligned}\hat{f}_1(y) &= \int_{A_K^+} f_1(t)X_y(-t)dm_A(t) = \int_{A_K^+} f(xt)X_y(-t)dm_A(t)\\ &= \int_{A_K^+} f(t)X_y(-tx^{-1})V^{-1}(x)dm_A(t)\\ &= V^{-1}(x)\int_{A_K^+} f(t)X_{y/x}(-t)dm_A(t)\\ &= V^{-1}(x)\hat{f}(y/x),\end{aligned}$$

and this leads, with the use of part (iii) of the Corollary to Proposition 6.23, to the asserted equality in view of Theorem VIII of Appendix I. □

Thus the inner integral in (6.12) becomes

$$\begin{aligned}&\int_E \chi_a(j)\left(V(tj)^{-1}\sum_{b\in A_0}\hat{f}(b/tj) - f(0)\right)d\mu_J(j)\\ &\qquad = \frac{1}{t}\int_E \chi_a(j)\sum_{b\in I_0} g_0(b/tj)d\mu_J(j)\\ &+ \frac{1}{t}\hat{f}(0)\int_E \chi_a(j)d\mu_J(j) - f(0)\int_E \chi_a(j)d\mu_J(j),\end{aligned}$$

and so B_2 turns out to be the sum of three integrals:

$$\begin{aligned}B_{21} &= \int_0^1 t^{s-2}\int_E \chi_a(j)\sum_{b\in I_0} g_0(b/tj)d\mu_J(j)dt,\\ B_{22} &= \hat{f}(0)\int_0^1 t^{s-2}dt\int_E \chi_a(j)d\mu_J(j), \quad \text{and}\\ B_{23} &= -f(0)\int_0^1 t^{s-1}dt\int_E \chi_a(j)d\mu_J(j),\end{aligned}$$

which we shall now evaluate separately. The first of them is similar in nature to B_1. Indeed, since χ_a is trivial on I_0, and every element of J_K can be uniquely written in the form bj with $b \in I_0$ and $j \in E$, we get

$$\begin{aligned}B_{21} &= \int_0^1 t^{s-2}\int_{J_K} g_0(1/tj)\chi_a(j)d\mu_J(j)dt\\ &= \int_{A_2} g_0(1/x)V(x)^{s-1}\chi_a(x/V(x))dm_I(x)\\ &= \int_{A_1} g_0(x)V(x)^{1-s}\chi_{a^{-1}}(x/V(x))dm_I(x),\end{aligned}$$

thus has the same form as B_1, and the same argument as used for B_1 shows that B_{21} defines an entire function.

To evaluate B_{22} and B_{23} observe that if χ_a is trivial on J_K, then Lemma 6.37 gives

$$\int_E \chi_a(j)d\mu_J(j) = \mu_J(E) = h\kappa,$$

and in other cases this integral vanishes.

Now note that with our choice of characters χ_a, if such character is trivial on J_K, then it is trivial on the full idele group I_K, since we have

$$\chi_a(x) = V(x)^{it} = \prod_v v(x_v)^{it}$$

with a suitable t, but in view of our normalization (Lemma 6.34) this implies $t = 0$. We arrive thus at the equality

$$\begin{aligned} Z(g, s, \chi_a) = &\int_{A_1} g(x)V(x)^s\chi_a(x)dm_I(x) \\ &+ \int_{A_1} g_0(x)V(x)^{1-s}\chi_{a^{-1}}(x)dm_I(x) \\ &+ \epsilon\left(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}\right)h\kappa, \end{aligned} \tag{6.13}$$

where

$$\epsilon = \begin{cases} 1 & \text{if } \chi_a = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and we see that the first two summands on the right-hand side are entire functions of s. This establishes the assertions (i) - (iii), and since (6.13) implies that the zeta-function $Z(g, s, \chi_a)$ is bounded in every fixed vertical strip, we obtain (v).

To prove the functional equation it suffices now to observe that the equality

$$\begin{aligned} Z(g_0, 1-s, \chi_{a^{-1}}) = &\int_{A_1} g_0(x)V(x)^{1-s}\chi_{a^{-1}}(x)dm_I(x) \\ &+ \int_{A_1} g(-x)V(x)^s\chi_a(x)dm_I(x) \\ +\epsilon\left(\frac{-f(0)}{s} + \frac{\hat{f}(0)}{s-1}\right)&h\kappa, \end{aligned}$$

follows from (6.13), and since the second integral remains unchanged after we substitute $-x$ for x, one sees immediately that this zeta function coincides with $Z(g, s, \chi_a)$. □

In the next chapter we shall apply this theorem to various functions f to obtain classical results of Riemann and Hecke

6.3. Notes to Chapter 6

1. The first to apply the $\mathfrak{p}$-adic approach to algebraic numbers was Hensel, who as early as 1894 demonstrated the power of this approach while solving a problem of Dedekind concerning the discriminant (Hensel [94a,b], [97a,b]). A systematic application of this method was outlined in Hensel [97c], [05a], [07], [13], [18]. Quadratic fields were treated in Hensel [14a] (cf. Bauer [22], Wahlin [15a]). Application to the factorization of prime ideals in various extensions can be found in Bauer [36], Bauer, Chebotarev [28], Hensel [21a,b], Ore [27], Rella [24a], Wahlin [15b], [22].

2. The applicability of $\mathfrak{p}$-adic numbers to the theory of quadratic forms was established by Hasse [23a,b], [24a,b] (cf. Hasse [62] for historical remarks), who proved that two such forms over an algebraic number field K are equivalent if and only if they are equivalent over every completion of K, and, moreover, a quadratic form F with coefficients in K represents a given element $a \in K$ if and only if F represents a in every completion of K (cf. Cassels [59a], O'Meara [63], Siegel [41], Springer [57]).

One says that for a given statement the *Hasse principle* holds, provided it is true in a field K if and only if it is true in every completion of K. It has been noted by Witt [35] that the Hasse principle fails for the solvability of the equation $x^2 + y^2 = a$ in fields of algebraic functions. It fails also for zeros of cubic forms, even over $\mathbb{Q}$, as shown by Selmer [51], who produced the example $3x^3 + 4y^3 + 5z^3$, which has non-trivial zeros in every completion of $\mathbb{Q}$, but not in $\mathbb{Q}$. See also Bremner [78], Cassels, Guy [66], Mordell [65], Selmer [53], Swinnerton-Dyer [62].

For quintic forms the Hasse principle also fails (Fujiwara [72]), as well as for certain other classes of forms (Birch, Swinnerton-Dyer [75], Fujiwara, Sudo [76], Manin [71]). Iskovskikh [71] showed that it fails also for common zeros of two quadratic forms, however, as shown in Waterhouse [76], it holds for the equivalence of such pairs.

An important example of the validity of this principle is the *Hasse Norm Theorem* (HNT) proved in Hasse [31d] (for earlier special cases see Furtwängler [04], [09], Hilbert [97, Satz 167], [99]). To state this result let $X(L/K)$ be the set of all elements of K^* which are norms in every local extension L_w/K_v, where v ranges over all valuations of K and w over all prolongations of v to L. Trivially one has $N_{L/K}(L^*) \subset X(L/K)$, and Hasse's theorem asserts that if L/K is cyclic, then we have equality here. For another proof see Gold [77]. The factor group $\mathfrak{K}(L/K) = X(L/K)/N_{L/K}(L^*)$ has been introduced by Scholz [36], who related it to Schur's multiplier (Schur [04]) of the Galois group of L/K. The group $\mathfrak{K}(L/K)$, called the *knot group* of L/K, has been studied later by Jehne [79], who also considered several related groups (see also Heider [80], [81], [84], Razar [77], Steckel [82a]).

For non-cyclic extensions Hasse's norm theorem may fail, as noted already in Hasse [31d], however, there are classes of extensions for which it is true.

This happens, e.g., for all extensions of prime degree (Bartels [81b], for the cubic case see Tasaka [70]), for extensions with a generalized quaternion group of order not divisible by 8 as Galois group (Arnaudon [76]), and also for all extensions, whose normal closure has a dihedral Galois group (Bartels [81a]). For other classes of fields see Garbanati [75], [77], [78a,b], Gerth [77a,b], [78], Gurak [78a,b], [80], Hamada [83], M.Horie [91], [93], Kagawa [95], Leep, Wadsworth [92], Platonov, Drakokhrust [85], Scholz [36].

Lorenz [80] proved that if L/K is normal, then there exists a normal extension M/K, containing L, such that all local norms of M/K become global norms in L/K. See also Lorenz [82], and Opolka [80a,b], [82], [84].

For other results concerning HNT see K.Amano [77], [79], Leep, Wadsworth [89], Opolka [87]. An application to diophantine equations was given by J.H.Smith [75]. For analogous questions concerning infinite extensions see Heider, and for units units see Gold [77] and Nakagoshi [75]. For a survey of questions related to HNT see Jehne [82].

Several other examples of Hasse's principle were given in Cantor, Roquette [84], Colliot-Thélène, Coray, Sansuc [80], Colliot-Thélène, Sansuc [82], Dress [65], Hasse [32], Hijikata [63], Landherr [36], Noether [33], O'Meara [59], Opolka [81], Pezda [03], Scharaschkin [99], Waterhouse [77], [78]. See also Chap. II.6 in the book of G.Gras [03].

3. The ramification groups were introduced by Hilbert [94a] directly, without the use of $\mathfrak{p}$-adic fields. For particular classes of fields they were studied in Dribin [37], Hasse [30b], Porusch [33], Rosenblüth [34].

In addition to papers on that topic quoted in Chap. 5 let us mention Herbrand [30a], Krasner [35], Speiser [19] and van der Waerden [34].

Corollary 2 to Proposition 6.8 was proved first in Chebotarev [29], Corollary 1 to Proposition 6.9 appears in McCulloh [66], and Corollary 2 is due to Netto [83], [84]. Theorem 6.11 was first proved by Wiman [99], and rediscovered later by Westlund [12]. For another proof see Albis-Gonzalez [73]. (In the first edition of this book the treatment of the case (v) of Theorem 6.11 was incomplete.) Generators of the group $G(I)$ in the case when it is cyclic are called *primitive roots* mod I. The analogue of *Artin's conjecture* on primitive roots states that every non-zero and non-unit element of R_K, which is not a square, is a primitive roots for infinitely many prime ideals of R_K. It has been shown by Lenstra,Jr. [77b] that this conjecture follows from the General Riemann Hypothesis. For other results on this conjecture see Egami [81], Hinz [84], [86] and Narkiewicz [87]. Primitive roots α mod $\mathfrak{P}$ with minimal $|N_{K/\mathbb{Q}}(\alpha)|$ were studied in Hinz [83a,b,c].

Finite commutative rings with a cyclic group of units were described by Gilmer [63b]. For other proofs see C.W.Ayoub [69], Pearson, Schneider [70], Raghavendran [70].

The structure of the group $G(\mathfrak{P}^n)$ was determined in Hensel [16b], [17], Nakagoshi [79], Takenouchi [13]. For particular cases see Dirichlet [41a], Halter-Koch [72a], Ranum [10]. The multiplicative semigroup of the ring

R_K/I for an arbitrary ideal I was described in Rieger [64]. An algorithm to determine the structure of its maximal subgroup gave Heß, Pauli, Pohst [03].

Proposition 6.13 had a wrong formulation in the first edition of this book. This was noticed by Lewittes [83], who computed the number of real primitive characters mod $\mathfrak{P}^k$,

4. Gaussian sums in the case of $K = \mathbb{Q}$ go back to Gauss and Lagrange, and in the general case there were introduced by Hecke [19] in the case of quadratic fields and by Hasse [51a] in the general case. See also Hasse [52b], [54a], Kubota [60]. A general theory of Gaussian sums in rings was developed by Lamprecht [53], [57].

Theorem 6.16 is due to Gauss [11], and the proof given by us was found by Waterhouse [70]. There are more than 25 proofs of that theorem, all listed in the survey of Berndt and Evans [81].

Theorem 6.17 was obtained independently by S.Chowla [62] and Mordell [62]. We reproduced Mordell's proof. See Evans [77], Funakura [92], Yokoyama [64] for generalizations. Explicit formulas for Gaussian sums with cubic and quartic characters in terms of elliptic functions were given in Matthews [79] (see also Barkan [90], Ito [89], Loxton [74a], [78], McGettrick [72], K.Yamamoto [65].)

There was a conjecture, originating in Kummer [42], [46], stating that if $p \equiv 1 \pmod 3$ runs over primes, then the arguments of Gaussian sums associated with a cubic character mod p are non-uniformly distributed on the unit circle. This was disproved by Heath-Brown and Patterson [79] (for an exposition of the proof see Venkov, Proskurin [82]). The same holds also for Gaussian sums of higher orders (Patterson [87].

Gaussian sums related to characters mod p^n with $n \geq 2$ are easier to handle, and can be evaluated explicitly as shown by Odoni [73a] (see also Mauclaire [83]).

Various relations between Gaussian sums, including important reciprocity theorems, were given in Barner [67], Davenport, Hasse [34], Hecke [19], Kubota [60], [61], [63], Kunert [35], Mordell [22a], L.H.Schmid [36], K.Yamamoto [66].

Gaussian sums were used in Hasse [40], [48a] and Bergström [44] for the study of class numbers. The role of Gaussian sums in the arithmetic of Abelian extensions of $\mathbb{Q}$ was emphasized by Leopoldt [62].

The full story of Gaussian sums over the rational field is given in the book of Berndt, Evans and Williams [98].

5. Theorem 6.18 was stated by Kronecker [53], [77], and its first proof (not quite complete) was published by H.Weber [86]. We presented the proof of Shafarevich [51] (see also Washington [82]). For other proofs see Chebotarev [24], Delaunay [23], Ghate [00], M.J.Greenberg [74], Hilbert [96], [97], Lubelski [39], Mertens [06], Riese [98], Speiser [19], Steinbacher [11], H.Weber [07],

Yamamoto, Onuki [75], Zassenhaus [68]. Neumann [81b] gave two proofs along the lines of Kronecker and Weber, discussing also other proofs.

An analogue for Abelian extensions of imaginary quadratic fields has been conjectured by Kronecker and proved, in a modified form by H.Weber [96b], [97] and Fueter [05] (cf. Fueter [11], [14], [24], Hasse [27], Hecke [17b], Ramachandra [64], Takagi [20]). The case of real quadratic fields was treated in Shintani [78].

An analogue of Theorem 6.18 for the field of rational functions in one variable over a finite field has been obtained by Hayes [74], and Drinfeld [74] did this for finite extensions of such fields. Drinfeld's proof has been simplified in Hayes [79]. See also the survey by Goss [80].

6. The question of the existence of a cyclic extension L/K of an algebraic number field K with prescribed local extensions $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, for $\mathfrak{p}$ lying in a given finite set S, was first considered by Grunwald [33]. However, it was pointed out by S.Wang [48] that there is a case in which Grunwald's argument does not apply. An improved version was obtained independently by Hasse [50b] and S.Wang [50a], and the final result is called the *Grunwald-Hasse-Wang theorem*. For other proofs see Artin, Tate [68], Neukirch [74b], and for a sharpening see Tomanov [88]. An analogous result holds for arbitrary Abelian extensions (Hasse [50b], S.Wang [50b]), and, more generally, for extensions with nilpotent Galois groups (Neukirch [73]). Cf. Miki [78], Neukirch [74c], Saltman [84]. In general it is not possible to prescribe the local behaviour in the case of S infinite. For example, there are no septic fields, ramified only at one prime $p = 2, 3, 5$, there are four such fields, ramified only at $p = 7$ (Bruegeman [01]), and there are 10 septic fields ramified only at $p = 2$ and 3 (Jones, Roberts [03]).

7. Ideles were introduced by Chevalley [36a], who used them for his reformulation of the class-field theory (Chevalley [40]). Adeles occur first in Artin, Whaples [45], where they were called valuation vectors.

For the topological properties of adeles and ideles see Artin, Tate [68], Iwasawa [53a]. The paper of Iwasawa contains the following characterization of the ring of adeles: if R is a semi-simple commutative locally compact ring with a unit element, neither compact nor discrete, and there is a discrete field $K \subset R$ with the same unit element and the factor-group R^+/K^+ is compact, then R is the ring of adeles either of an algebraic number field, or of a field of algebraic functions in one variable over a finite field of constants (in the latter case one defines the ideles in an analogous way).

Examples of non-isomorphic fields with isomorphic adele rings were given in Jacobson, Vélez [85], Komatsu [78], [84]. A criterion for this phenomenon in terms of norm-forms was given by Meyer, Perlis [79].

An exposition of the theory of adeles was given by A.Robert [74].

The structure of $D(K)$ was determined by Weil [51], and other proofs were given in Artin [56], Kobayashi [83]. One proves in the class-field theory that

the quotient group $C(K)/D(K)$ is topologically isomorphic to $Gal(K^{ab}/K)$, K^{ab} being the maximal Abelian extension of K.

A characterization of characters of $C(K)$ among those of the full idele group was given in Gurevich [71]. We shall encounter these characters again in the next chapter.

Certain subgroups of I_K were studied in Furuta [66], Masuda [57], Miyake [80b].

The idele class-groups of imaginary quadratic fields were described by Onabe [78], who gave also examples of fields with isomorphic idele class-groups, but distinct ideal class-groups (e.g. $K = \mathbb{Q}(\sqrt{-d})$ with $d = 8$, 20 ,23, 47 and 71). Komatsu [74] showed that if $Gal(\hat{Q}/K) \sim Gal(\hat{Q}/L)$ (where $\hat{Q}$ is the algebraic closure of $\mathbb{Q}$), then $I_K \sim I_L$, and in [76c] he produced examples to show that the converse implication fails for adele rings in place of idele groups.

8. The discriminant $\partial(L/K)$ was introduced by Fröhlich [60b], [61], who applied this notion in [60c,d]. Proposition 6.30 is due to to him. Normal extensions L/K with $\partial(L/K) \in I_K^2/U_K^2$ were characterized in Maurer [78a], [79] as those for which the 2-Sylow subgroup of the Galois group is non-cyclic.

Hecke [23] proved that the class of $D_{L/K}$ in $H(L)$ is a square. This immediately implies Theorem 6.31. Other proofs of Theorem 6.31 were given in Armitage [67], Fröhlich [60b], Knebusch, Scharlau [71], Weil [67]. It holds in every Dedekind domain (Armitage [67]), however the class of the different is not necessarily a square in this more general situation, as shown in Fröhlich, Serre, Tate [62]. If the extension L/K is normal of odd degree, then the different $D_{L/K}$ is itself a square of a certain ideal $I_{L/K}$. See Erez [91] for properties of $I_{L/K}$.

The results of Sect.5, in particular Theorem 6.36 are due to Tate [50]. A more general class of zeta-functions was considered by Ono [70].

9. A $\mathfrak{p}$-adic analogue of the regulator matrix was introduced by Leopoldt [62], who conjectured that its rank is independent on $\mathfrak{p}$, and coincides with the rank of the usual regulator matrix. This was shown to be true for Abelian fields by Brumer [67] (see also Ax [65]), and other special cases were settled in Bertrandias, Payan [72], G.Gras [72a], Kuzmin [81], Miyake [82]. In the general case Waldschmidt [81] proved that the rank of the $\mathfrak{p}$-adic regulator is $\geq (r_1(K) + r_2(K) - 1)/2$. For other results concerning Leopoldt's conjecture see Gillard [79d], Iwasawa [65]. More information can be found on the book of G.Gras [03].

Diophantine approximations and geometry of numbers in the ring of adeles as well as the analogues of Pisot numbers were studied in Bertrandias [65], Cantor [65], Decomps-Guilloux [65a,b], [70], Grandet-Hugot [66], [75], McFeat [71], Senge [67].

EXERCISES

1. Characterize wildly ramified extensions L/K with $T_{L/K}(R_L) = R_K$ in terms of factorization of prime ideals.

2. Determine the inertia and ramification groups for the following extensions $K/\mathbb{Q}$:
(a) $K/\mathbb{Q}$ quadratic,
(b) $K = \mathbb{Q}(\zeta_p)$ with prime p,
(c) $K = \mathbb{Q}(\sqrt{i})$.

3. Determine the structure of the group $G(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal in R_K with $f_{K/\mathbb{Q}}(\mathfrak{p}) \geq 2$.

4. Determine all natural numbers n for which the group $G(n\mathbb{Z})$ has primitive characters of a given order k.

5. Let L/K be a finite extension of an algebraic number fields and define the idele norm map by the formula

$$N_{L/K}(\langle a_v \rangle_v) = \left\langle \prod_{v \text{ over } w} N_{L_v/K_w} \right\rangle_w .$$

Prove that $N_{L/K} : I_L \longrightarrow I_K$ is a continuous homomorphism which agrees on principal ideal with the usual norm map from L^* to K^*.

6. Prove an analogue of the preceding exercise for an appropriately defined trace map from A_L to A_K.

7. (Weil [39]) (i) Estimate the number of principal adeles $\langle a_v \rangle$, satisfying $v(a_v) \leq T_v$, where T_v are given non-negative real numbers of which only finitely many are non-zero.

(ii) Let $a \in K$ and let $\langle a_v \rangle$ be the corresponding principal idele. For $v \in S_\infty$ put

$$T_v(a) = \begin{cases} a_v & \text{if } v \text{ is real,} \\ a_v + \overline{a_v} & \text{otherwise,} \end{cases}$$

and for remaining v's put $T_v(a) = T_{K_v/\mathbb{Q}_p}(a_v)$, where p is the unique rational prime with $v(p) \neq 1$. Moreover for $v \in S_\infty$ let $t_v(a) = -T_v(a)$ and for $v \notin S_\infty$ let $t_v(a)$ be a rational number r such that $T_v(a) - r \in R_v$.

Prove that for all $a \in K$ the number $\sum_v t_v(a)$ is a rational integer.

7. Analytical Methods

7.1. The Classical Zeta-Functions

1. In this section we introduce the Dirichlet series defining the Dedekind zeta-function, and also some other kinds of zeta-functions, including Dirichlet's L-functions, and derive the functional equations for them. Our arguments will be based on the results of Chap. 6. Subsequent sections are devoted to asymptotic distribution of ideals and prime ideals. We shall use the tauberian theorem of Delange, an account of which is given in Appendix II, as well as complex integration in its simplest form. We adopt the convention that $\sum_I$ and $\sum_{\mathfrak{p}}$ denote summations over all non-zero ideals, respectively all non-zero prime ideals of the considered algebraic number field. We shall also denote[2] by σ, t the real, respectively the imaginary part of the complex variable s.

We start with Dedekind's zeta-function of an algebraic number field K, which is defined by

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s}. \tag{7.1}$$

To obtain its properties we need an analogue of Euler product formula for ideals:

Lemma 7.1. *Let f be a complex-valued function defined on the set of all non-zero ideals of R_K and assume that it is multiplicative, i.e., for relatively prime ideals I, J we have $f(IJ) = f(I)f(J)$. Assume, moreover, that the series*

$$G(f,s) = \sum_I \frac{f(I)}{N(I)^s}$$

converges absolutely in a certain half-plane $\sigma > C$. Then in that half-plane we have the equality

$$G(f,s) = \prod_{\mathfrak{p}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}}.$$

[2] This peculiar notation goes back to Riemann's memoir on prime numbers. A legend says that he did not know the letter τ, but it was rather a printers fault.

Proof : For a real positive T denote by A_T the set of all ideals of R_K whose prime ideal divisors have their norms not exceeding T. Then obviously we have

$$\prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \le T}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} = \sum_{I \in A_T} \frac{f(I)}{N(I)^s},$$

hence the difference

$$\left| \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \le T}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} - \sum_{\substack{I \\ N(I) \le T}} \frac{f(I)}{N(I)^s} \right|$$

does not exceed

$$\sum_{\substack{I \\ N(I) > T}} \left| \frac{f(I)}{N(I)^s} \right|,$$

and this tends to zero. □

Proposition 7.2. *In the half-plane $\sigma > 1$ the series (7.1) converges absolutely, and the convergence is uniform in every compact subset of that half-plane, so $\zeta_K(s)$ is regular there. Moreover, in that half-plane the infinite product*

$$P(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

converges, and we have $P(s) = \zeta_K(s)$.

Proof : Let $[K : \mathbb{Q}] = n$. Since there are at most n prime ideals in R_K with a given norm, and every such norm is a prime power, the series $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-\sigma}$ is for $\sigma > 1$ absolutely convergent, and its convergence is uniform in every compact set, since it is majorized by the series

$$\sum_{q} \frac{n}{q^\sigma},$$

where q runs over all prime-powers in $\mathbb{Z}$. If $T > 0$, then

$$\sum_{\substack{I \\ N(I) \le T}} |N(I)^{-s}| \le \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \le T}} \left(1 + N(\mathfrak{p})^{-\sigma} + N(\mathfrak{p})^{-2\sigma} + \cdots\right),$$

but the series in brackets on the right-hand side does not exceed $1 + 3N(\mathfrak{p})^{-\sigma}$, and so

$$\sum_{\substack{I \\ N(I) \le T}} |N(I)^{-s}| \le \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \le T}} (1 + 3N(\mathfrak{p})^{-\sigma}) \le B,$$

with a constant B, because the series $3\sum_{\mathfrak{p}} N(\mathfrak{p})^{-\sigma}$ converges in our range uniformly in every compact set. This proves everything except the infinite

product representation of $\zeta_K(s)$, but this is an immediate consequence of Lemma 7.1. □

Corollary 1. *The function $\zeta_K(s)$ does not vanish in the half-plane $\sigma > 1$.*

Proof : No term of the infinite product for $\zeta_K(s)$ can vanish in this half-plane. □

The analogue $\mu_K(I)$ of the classical Möbius function is defined by

$$\mu_K(I) = \begin{cases} 1 & \text{if } I = R_K, \\ (-1)^k & \text{if } I \text{ is the product of } k \text{ distinct prime ideals,} \\ 0 & \text{if } I \text{ is divisible by the square of a prime ideal.} \end{cases}$$

One sees in exactly the same way as in the case of the usual Möbius function that

$$\sum_{J|I} \mu_K(J) = \begin{cases} 1 & \text{if } I = R_K, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 2. *The function $\zeta_K(s)^{-1}$ is regular for $\sigma > 1$, and we have there the equality*

$$\frac{1}{\zeta_K(s)} = \sum_I \frac{\mu_K(I)}{N(I)^s}.$$

Moreover, in the same range one has

$$|\zeta_K(s)^{-1}| \leq \zeta_K(\sigma).$$

Proof : The regularity follows from the preceding corollary and it remains to observe that

$$\sum_I \frac{\mu_K(I)}{N(I)^s} \cdot \zeta_K(s) = \sum_I \frac{\sum_{J|I} \mu_K(J)}{N(I)^s} = 1.$$

□

Corollary 3. *If $F(n)$ denotes the number of ideals of R_K with norm equal to n, then for $\sigma > 1$ one has*

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s}$$

and

$$|\zeta_K(s)| \leq \zeta(\sigma)^N,$$

where $N = [K : \mathbb{Q}]$, and $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ is the Riemann zeta-function.

Proof : The first assertion is obvious, and to obtain the second recall that if $d_N(n)$ denotes the number of representations of n as a product of N factors, then Lemma 4.9 gives $F(n) \leq d_N(n)$, hence

$$|\zeta_K(s)| \leq \sum_{n=1}^{\infty} \frac{F(n)}{n^\sigma} \leq \sum_{n=1}^{\infty} \frac{d_N(n)}{n^\sigma} = \zeta(\sigma)^N. \quad \square$$

2. Now we prove the main property of Dedekind's zeta-function, which was first established by Hecke [17a] with the use of the theory of theta-functions.

Theorem 7.3. *The function $\zeta_K(s)$ can be continued analytically to a meromorphic function having a unique simple pole at $s = 1$ with the residue $h\kappa$, κ being defined by* (6.8). *Moreover, if we put $N = [K : \mathbb{Q}]$, and*

$$A = \frac{1}{2^{r_2}\pi^{N/2}}\sqrt{|d(K)|},$$

then the function

$$\Phi(s) = A^2\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$$

satisfies the functional equation $\Phi(s) = \Phi(1-s)$.

Proof : We are going to apply Theorem 6.36 to the function $f = \prod_v f_v$, where for non-Archimedean v we choose for the function f_v the characteristic function of the ring R_v of integers of K_v, whereas for Archimedean v we put

$$f_v(x_v) = \begin{cases} \exp(-\pi x_v^2) & \text{if } v \text{ is real,} \\ \exp(-2\pi v(x_v)) & \text{if } v \text{ is complex.} \end{cases}$$

(Remember that for complex v we have $v(x) = |x|^2$.)

Let us now compute the Fourier transforms and zeta-functions of the functions f_v, corresponding to the quasicharacter v^s. In the real case we obtain without difficulty

$$\hat{f}_v(y_v) = \int_{-\infty}^{\infty} \exp(-\pi x_v^2 + 2\pi i x_v y_v)dx = \exp(-\pi y_v^2) = f_v(y_v)$$

and

$$\int_{\mathbb{R}^*} f_v(x_v)v(x_v)^2 d\mu_{\mathbb{R}}(x) = \int_{\mathbb{R}^*} \hat{f}_v(y_v)v(y_v)^s d\mu_{\mathbb{R}}(y) = \pi^{-s/2}\Gamma(s/2). \quad (7.2)$$

Similarly, in the complex case we get for $x_v = x + iy$, $y_v = a + bi$

$$\begin{aligned} \hat{f}_v(y_v) =& f_v(a+bi) = 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp(-2\pi(x^2+y^2) + 4\pi i(ax - by))dxdy \\ =& \exp(-2\pi(a^2+b^2)) = f_v(y_v), \end{aligned}$$

and

$$\begin{aligned}\int_{\mathbb{C}^*} f_v(x)v(x_v)^s d\mu_{\mathbb{C}}(x) &= 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp(-2\pi(x^2+y^2))(x^2+y^2)^{s-1}dxdy \\ &= 2\int_0^{\infty} dr \int_0^{2\pi} \exp(-2\pi r^2) r^{2s-1} d\varphi = \Gamma(s)\pi^{1-s} \\ &= \int_{\mathbb{C}^*} \hat{f}_v(y_v)v(y_v)^s d\mu_{\mathbb{C}}(y). \end{aligned} \tag{7.3}$$

For non-Archimedean v we obtain

$$\hat{f}_v(y_v) = \int_{K_v} f_v(x_v)\chi_{y_v}(-x_v)d\mu_v(x) = \begin{cases} N(D_v)^{-1/2} & \text{if } y_v \in D_v^{-1}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\chi_{y_v}(t) = X(ty_v)$, $X(t)$ being the standard character of K_v^+, and D_v is the different of the extension $K_v/\mathbb{Q}_p$. Moreover,

$$\begin{aligned}\int_{K_v^*} f_v(x_v)v(x_v)^s d\mu_v^*(x) &= \frac{N(\mathfrak{p}_v)}{N(\mathfrak{p}_v)-1}\int_{K_v} f_v(x_v)v(x_v)^{s-1}d\mu_v(x) \\ &= \frac{N(\mathfrak{p}_v)}{N(\mathfrak{p}_v)-1}\int_{R_v} v(x_v)^{s-1}d\mu_v(x)\end{aligned}$$

holds for $\sigma > 1$, $\mathfrak{p}_v$ being the prime ideal of R_v. If we fix a generator π_v of $\mathfrak{p}_v$, then we get, with $U = U(K_v)$,

$$\begin{aligned}\int_{R_v} v(x_v)^{s-1}d\mu_v(x) &= \sum_{j=0}^{\infty}\int_{\pi^j U} v(x_v)^{s-1}d\mu_v(x) \\ &= \sum_{j=0}^{\infty} N(\mathfrak{p}_v)^{-js}\int_U v(x_v)^{s-1}d\mu_v(x) \\ &= (1-N(\mathfrak{p}_v)^{-s})^{-1}\int_U d\mu_v(x) \\ &= \frac{N(\mathfrak{p}_v)-1}{N(\mathfrak{p}_v)}\frac{N(D_v)^{-1/2}}{1-N(\mathfrak{p}_v)^{-s}},\end{aligned}$$

because the equality

$$N(D_v)^{-1/2} = \int_{R_v} d\mu_v(x) = \sum_{j=0}^{\infty}\int_{\pi^j U} d\mu_v(x) = \sum_{j=0}^{\infty} N(\mathfrak{p}_v)^{-j}\int_U d\mu_v(x)$$

implies

$$\int_U d\mu_v(x) = \frac{N(\mathfrak{p}_v)-1}{N(\mathfrak{p}_v)N(D_v)^{1/2}}.$$

We have thus obtained the equality

$$\int_{K_v^*} f_v(x_v)v(x_v)^s d\mu_v^*(x) = N(D_v)^{-1/2}(1 - N(\mathfrak{p}_v)^{-s})^{-1}, \tag{7.4}$$

and similarly one gets

$$\int_{K_v^*} \hat{f}_v(y_v)v(y_v)^s d\mu_v^*(y) = N(D_v)^{s-1}(1 - N(\mathfrak{p}_v)^{-s})^{-1}. \tag{7.5}$$

Now we check that the function f satisfies the assumptions of Theorem 6.36. Since all functions f_v are continuous and integrable in K_v^+, and since almost all of them are equal to 1 on R_v, Lemma 2 of Appendix I shows that f is continuous, and, moreover, the equality

$$\int_{K_v} |f_v(x_v)| d\mu_v(x) = N(D_v)^{-1/2}$$

for non-Archimedean v shows that we can apply the Corollary to Lemma 2 of Appendix I to obtain the integrability of f. Moreover, Lemma 3 and the Corollary to Lemma 4 of the same appendix jointly with the equality

$$\int_{K_v} |\hat{f}_v(y_v)| dy_v = 1$$

show that the Fourier transform $\hat{f}$ is continuous and integrable, and one has

$$\hat{f}(\langle y_v \rangle) = \prod_v \hat{f}_v(y_v).$$

This shows that the condition (a) of Theorem 6.36 is satisfied, and we may turn to condition (b). Readers acquainted with Hecke's classical proof of our theorem, which was based on the properties of theta-functions, will recognize them hidden in the background of the verification which now follows.

Let $a = \langle a_v \rangle \in I_K$, $x = \langle x_v \rangle \in I_K$ and $t \in K = A_0$. We can write $f(a(x + t)) = P_1 P_2$, with

$$P_1 = \prod_{v \in S_\infty} f_v(a_v(x_v + t)), \quad P_2 = \prod_{v \notin S_\infty} f_v(a_v(x_v + t)).$$

It is immediate that we have

$$P_2 = \begin{cases} 1 & \text{if for } v \notin S_\infty \text{ one has } a_v(x_v + t) \in R_v, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, if we denote by F_v the embedding of K in K_v, and put

$$\eta_v = \begin{cases} 1 & \text{for real } v, \\ 2 & \text{for complex } v, \end{cases}$$

then we get

$$\sum_{t\in K} f(a(x+t)) = \sum_{t\in W(a,x)} \exp\left(-\pi \sum_{v\in S_\infty} \eta_v |a_v(x_v + F_v(t))|^2\right),$$

where

$$W(a,x) = \{t \in K : \ a_v(x_v + t) \in R_v \text{ for } v \notin S_\infty\}.$$

Now let C_1, C_2 be compact subsets of I_K and A_K, respectively, and put

$$W = \bigcup_{a\in C_1} \bigcup_{x\in C_2} W(a,x).$$

The compactness of C_1 and C_2 implies the existence of positive constants c_1, c_2, c_3 and a finite set S of normalized valuations such that for

$$(\langle a_v\rangle, \langle x_v\rangle) \in C_1 \times C_2$$

we have $v(a_v) = 1$ and $v(x_v)$ for $v \notin S$, and $c_1 \le v(a_v) \le c_2$, $v(x_v) \le c_3$ for $v \in S$. If v is non-Archimedean, and ν_v denotes the exponent of K_v, then with suitable b_1, b_2, b_3 we have $b_1 \le \nu_v(a_v) \le b_2$ and $\nu_v(x_v) \le b_3$. Now let π_v be the generator of the prime ideal of R_v, put

$$J = \prod_{v\in S\setminus S_\infty} \pi_v^{\min\{b_3, -b_2\}},$$

and observe that J is a fractional ideal containing W. In fact, if $t \in W$, then for some $\langle a_v\rangle \in C_1$ and $\langle x_v\rangle \in C_2$ we have for non-Archimedean v the inequality $\nu_v(a_v(x_v + t)) \ge 0$, hence for such v we get

$$\begin{aligned}\nu_v(t) =& \nu_v(x_v + t - x_v) \ge \min\{\nu_v(x_v), \nu_v(x_v + t)\} \\ &\ge \min\{\nu_v(x_v), -\nu_v(a_v)\} \ge \min\{b_3, -b_2\}\end{aligned}$$

for $v \in S$ and, similarly, $\nu_v(t) \ge 0$ for $v \notin S$.

It remains to prove that the series

$$\sum_{t\in J} \exp\left(-\pi \sum_{v\in S_\infty} \eta_v |a_v(x_v + F_v(t))|^2\right)$$

converges uniformly for $(\langle a_v\rangle, \langle x_v\rangle) \in C_1 \times C_2$. For this purpose let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis of J, so that every element $t \in J$ can be uniquely written in the form

$$t = \sum_{j=1}^{n} y_j \omega_j \quad (y_j \in \mathbb{Z}).$$

Our series becomes

$$\sum_{y_1,\ldots,y_n\in\mathbb{Z}} \left(-\pi \sum_{v\in S_\infty} \eta_v \Big|a_v(x_v + \sum_{j=1}^{n} y_j F_v(\omega_j))\Big|^2\right).$$

But our assumptions imply that $|a_v|$ is bounded from below by a positive constant, and $|x_v|$ is bounded from above. Hence the inner sum exceeds a constant multiple of $\sum_{j=1}^{n} y_j^2$, except for a finite number of terms depending only on C_2, and we see finally that our series is majorized by a constant multiple of

$$\left(\sum_{y=-\infty}^{\infty} \exp(-By^2) \right)^n$$

with a certain positive B, a series evidently convergent.

In the same way we deal with the second series occurring in the condition (b) of Theorem 6.36.

Condition (c) is in our case a consequence of the estimates

$$\sup_S \prod_{v \in S} \int_{K_v^*} |f_v(x_v)| v(x_v)^t d\mu_v^*(x) \leq (\pi^{-t/2}\Gamma(t/2))^{r_1} ((2\pi)^{1-t}\Gamma(t))^{r_2} \times |d(K)|^{-1/2} \prod_{v \notin S_\infty} (1 - N(\pi_v)^{-t})^{-1},$$

and

$$\sup_S \prod_{v \in S} \int_{K_v^*} |\hat{f}_v(y_v)| v(y_v)^t d\mu_v^*(y) \leq (\pi^{-t/2}\Gamma(t/2))^{r_1} ((2\pi)^{1-t}\Gamma(t))^{r_2} \times |d(K)|^{t-1} \prod_{v \notin S_\infty} (1 - N(\pi_v)^{-t})^{-1},$$

which follow from (7.2), (7.3), (7.4) and (7.5). The convergence of the product

$$\prod_{v \notin S_\infty} (1 - N(\pi_v)^{-t})^{-1}$$

is ensured by Proposition 7.2.

Thus we see that all conditions of Theorem 6.36 are satisfied by our function f. If we now define for $\sigma > 1$ the function Ψ by

$$\Psi(s) = \prod_{v \in S_\infty} \int_{K_v^*} f_v(x_v) v(x_v)^s d\mu_v^*(x) = \prod_{v \in S_\infty} \int_{K_v^*} \hat{f}_v(y_v) v(y_v)^s d\mu_v^*(y),$$

then, again using the equalities (7.2) - (7.5), we obtain

$$Z(f, s) = \Psi(s)\zeta_K(s)|d(K)|^{-1/2}$$

and

$$Z(\hat{f}, s) = \Psi(s)\zeta_K(s)|d(K)|^{s-1}.$$

By Theorem 6.36 these two zeta-functions can be continued analytically to meromorphic functions, whose only poles can lie at $s = 0$ or $s = 1$. Furthermore, Ψ satisfies the functional equation

$$\Psi(s)\zeta_K(s)|d(K)|^{-1/2} = \Psi(1-s)\zeta_K(1-s)|d(K)|^{-s}. \tag{7.6}$$

One checks without difficulty that this is just the equation occurring in the formulation of the theorem. At $s = 1$ the function $Z(f, s)$ has a simple pole, and since $\Psi(1) = 1$ we get $\hat{f}(0) = |d(K)|^{-1/2}$, which shows that $\zeta_K(s)$ has a simple pole at $s = 1$ with residue $h\kappa$. At $s = 0$ the function $\Psi(s)\zeta_K(s)$ has a simple pole, but $\Psi(s)$ has there a pole of order $r_1 + r_2$, and so we see that $\zeta_K(s)$ is regular at $s = 0$. This establishes all assertions of our theorem. □

Corollary 1. *For $s \notin \{0, 1\}$ one has*

$$\int_{V(x)\geq 1} \left(\hat{f}(x)V(x)^s + f(-x)V(x)^{1-s}\right) dm_I(x) + h\kappa\left(\frac{1}{s-1} - \frac{1}{s\sqrt{|d(K|}}\right)$$
$$= \zeta_K(s)|d(K)|^{s-1}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\pi^{-sr_1/2}(2\pi)^{r_2(1-s)}.$$

Proof : Apply the equality (6.13) to the function $\hat{f}$ and $q_a = 1$, remembering that $\hat{\hat{f}}(x) = f(-x)$. □

Corollary 2. *If $h\kappa$ denotes the residue of $\zeta_K(s)$ at 1, then for $s > 1$ we have*

$$h\kappa \leq D^{s-1/2}\frac{s(s-1)}{s\sqrt{D}+1-s}\zeta_K(s)\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\pi^{-sr_1/2}(2\pi)^{r_2(1-s)},$$

with $D = |d(K)|$.

Proof : Apply the preceding corollary, noting that the integrand is non-negative. □

Corollary 3. *For $0 < a \leq 1$ we have*

$$h\kappa \leq 2^{1+n}(D\pi^{-n/2})^a a^{1-n} \leq 2^{1+n}D^a a^{1-n},$$

where $n = [K : \mathbb{Q}]$ and $D = |d(K)|$.

Proof : Put in the preceding corollary $s = 1 + a$, and observe that

$$\Gamma((1+a)/2)^{r_1}\Gamma(1+a)^{r_2}\pi^{-(1+a)r_1/2}(2\pi)^{-ar_2} \leq \pi^{-an/2}2^{-ar_2} < \pi^{-an/2},$$

because of

$$\Gamma((1+a)/2) \leq \Gamma(1/2) = \sqrt{\pi}, \quad \text{and} \quad \Gamma(1+a) \leq \Gamma(2) = 1.$$

Corollary 3 to Proposition 7.2 gives $\zeta_K(x) \leq \zeta(x)^n$ for $x > 1$, and in view of the inequality

$$\zeta(x) = \sum_{n=1}^{\infty}\frac{1}{n^x} \leq 1 + \int_1^{\infty}\frac{dt}{t^x} = \frac{x}{x-1} \leq \frac{2}{x-1},$$

holding for $1 < x \leq 2$ we get $\zeta_K(1+a) \leq (2/a)^n$.

The assertion results now by observing that

$$\frac{s(s-1)\sqrt{D}}{s\sqrt{D}+1-s} \leq 2(s-1). \quad \square$$

Corollary 4. *For every field K of degree n we have*

$$h(K)R(K) = O(\sqrt{D}\log^{n-1} D),$$

with $D = |d(K)|$, the implied constant depending only on n.

Proof : In the last corollary put $a = 1/\log D$. This leads to $h\kappa \leq C\log^{n-1} D$ with a certain C, depending only on n. Using the equality

$$h(K)R(K) = w(K)h(K)\kappa\sqrt{D}2^{-r_1-r_2}\pi^{-r_2},$$

with $w(K)$ being the number of roots of unity contained in K, we arrive at our assertion, because there are only finitely many roots of unity of a given degree. $\square$

Corollary 5. *If K and L are algebraic number fields with the same Dedekind zeta-function, then $[K:\mathbb{Q}] = [L:\mathbb{Q}]$, $d(K) = d(L)$, $r_1(K) = r_1(L)$, $r_2(K) = r_2(L)$, and*

$$\frac{h(K)R(K)}{w(K)} = \frac{h(L)R(L)}{w(L)}.$$

Proof : If $\zeta_k = \zeta_L$, then Corollary 3 to Proposition 7.2 shows that for every N the numbers of ideals of norm N in R_K and R_L coincide. For prime n these numbers are bounded by the corresponding degrees, and by Theorem 4.37 these bounds are attained. This implies $[K:\mathbb{Q}] = [L:\mathbb{Q}]$. If now Φ_K and Φ_L are functions appearing in Theorem 7.3, corresponding to K and L, and A_K, A_L are the respective constants, then

$$\Phi_K(s) = \Phi_K(1-s) = A_K^s\Gamma(s/2)^{r_1(K)}\Gamma(s)^{r_2(K)}\zeta_K(s)$$

and

$$\Phi_L(s) = \Phi_L(1-s) = A_L^s\Gamma(s/2)^{r_1(L)}\Gamma(s)^{r_2(L)}\zeta_L(s),$$

and division yields

$$\begin{aligned}&(A_K/A_L)^{2s-1}\Gamma(s/2)^{r_1(K)-r_1(L)}\Gamma(s)^{r_2(K)-r_2(L)}\\ &= \Gamma((1-s)/2)^{r_1(K)-r_1(L)}\Gamma(1-s)^{r_2(K)-r_2(L)}.\end{aligned}$$

The right-hand side is regular in a neighbourhood of $s = 0$, and since $\Gamma(s)$ has a pole there, we must have $r_1(K) + r_2(K) = r_1(L) + r_2(L)$, and since the degrees of K and L coincide we get $r_1(K) = r_1(L)$ and $r_2(K) = r_2(L)$.

Therefore $(A_K/A_L)^{2s-1} = 1$ holds for all s, leading to $A_K = A_L$, which in turn implies $|d(K)| = |d(L)|$. By Proposition 2.15 the signs of the discriminants coincide, hence $d(K) = d(L)$. The last assertion follows by comparing the residues of ζ_K and ζ_L at $s = 1$. □

Corollary 6. *If K is either $\mathbb{Q}$, or an imaginary quadratic field, then $\zeta_K(0) \neq 0$. Otherwise $\zeta_K(s)$ has a zero of order $r_1 + r_2 - 1$ at $s = 0$.*

Proof : Apply the functional equation and the fact that $\Gamma(s)$ has a simple pole at $s = 0$. □

3. We now introduce a class of multiplicative complex-valued functions defined on the group $G(K)$ of all fractional ideals of K, which we shall call *Hecke characters*. Let X be a quasicharacter of the idele class-group $C(K)$, i.e. a quasicharacter of I_K, trivial on J_K. According to Theorem IX of Appendix I we can write

$$X(\langle x_v \rangle) = \prod_v X_v(x_v),$$

where X_v is a quasicharacter of K_v^*, equal to unity on $U(K_v)$ for almost all v's.

Let Ω be, as in the previous chapter, a fixed set of normalized inequivalent valuations, and let S be a finite subset of Ω, containing S_∞ as well as all those v's for which X_v is non-trivial on $U(K_v)$. For $v \notin S$ the value $X_v(x_v)$ depends only on $v(x_v)$, and thus we can consider X_v as a quasicharacter of the group of all fractional ideals of K_v, which is an infinite cyclic group. Define now a function χ on $G(K)$ by putting for all prime ideals $\mathfrak{p}$ of R_K

$$\chi(\mathfrak{p}) = \begin{cases} X_v(\mathfrak{p}_v) & \text{if } \mathfrak{p}R_v = \mathfrak{p}_v, v \notin S, \\ 0 & \text{otherwise,} \end{cases}$$

and extending it to $G(K)$ by multiplicativity.

The restriction of χ to the subgroup of $G(K)$ generated by the prime ideals $\mathfrak{p}_v$ $(v \notin S)$ is a quasicharacter. Although χ itself is not a quasicharacter (except when $S = S_\infty$), since it can assume the value zero, we call it a *Hecke character*. If X is a character of $C(K)$, then χ is called a *proper Hecke character*. The set S is called the *exceptional set of* χ.

If X is a character satisfying the normalization condition stated in Lemma 6.34, then χ is called a *normalized Hecke character*. Note that in view of (6.7) every Hecke character χ may be uniquely represented in the form

$$\chi(I) = \chi_1(I)N(I)^s, \tag{7.7}$$

where χ_1 is a normalized (hence proper) Hecke character and $s \in \mathbb{C}$. Moreover, the character χ is proper if and only if $\sigma = 0$.

The formula (7.7) shows that in most questions one can restrict attention to proper Hecke characters.

Our next aim is to give an intrinsic characterization of Hecke characters. For this purpose we shall consider a slightly more general situation. Let G be a complete metric Abelian group, and let S be a finite set of normalized valuations of K, containing S_∞. Denote by $G(K;S)$ the group of all fractional ideals of K, whose factorization into prime ideals contains no factors corresponding to $v \in S \setminus S_\infty$. Moreover, for any fractional ideal I of K denote by I_S the S-free part of I, i.e., the unique ideal of $G(K;S)$ for which we have $I = I_S I'$, all prime factors of I' corresponding to $v \in S$. A homomorphism $f : G(K;S) \longrightarrow G$ will be called *admissible*, if for every neighbourhood U of unity in G there exists a positive ϵ such that for every $x \in K^*$, satisfying $v(x-1) < \epsilon$ for $v \in S$, the element $f((xR_K)_S)$ lies in U.

It will turn out that proper Hecke characters are exactly those homomorphisms of $G(K)$ into T which are induced by admissible homomorphisms of the groups $G(K;S)$. This is implied by the next result, which we shall later use also in the case of G finite. In its proof, and also in the sequel, we shall utilize a convenient extension of the notion of congruence: if $I = \prod_v \mathfrak{p}_v^{a_v}$ is the canonical factorization of an ideal I of R_K, and x, y are elements of K, then we shall write $x \equiv y \,(\mathrm{mod}\ I)$ to indicate that for all $\mathfrak{p}_v | I$ one has $\nu_v(x-y) \geq a_v$.

Theorem 7.4. *Let G be a complete metric Abelian group possessing a neighbourhood of the unit element not containing any non-trivial subgroup of G. Then a homomorphism $f : G(K;S) \longrightarrow G$ is admissible if and only if there is a continuous homomorphism $F : I_K \longrightarrow G$, trivial on I_0, and such that for every idele $x = \langle x_v \rangle$ with $x_v = 1$ for $v \in S$ we have*

$$F(x) = f \circ g(x),$$

where g is the canonical map $I_K \longrightarrow I_K/U_K = G(K)$.

If such an F exists, then it is unique.

Proof : We deal with the sufficiency part first. Let F satisfy all stated conditions, and write it, by Theorem IX of Appendix I, as $F(x) = \prod_v F_v(x_v)$, F_v being continuous homomorphisms of K_v^* into G, almost all of them trivial on $U(K_v)$. Since G does not have arbitrarily small subgroups, to each non-Archimedean $v \in S$ there corresponds an ideal $\mathfrak{f}_v$ of R_v such that the congruence $x_v \equiv 1 \,(\mathrm{mod}\ \mathfrak{f}_v)$ implies $F_v(x_v) = 1$. Therefore, if $v(x-1)$ is sufficiently small for each $v \in S \setminus S_\infty$, then

$$\prod_{v \in S \setminus S_\infty} F_v(x_v) = 1.$$

But then we have for $x \in K^*$

$$1 = F(x) = \prod_{v \in S_\infty} F_v(x) \cdot f((xR_K)_S),$$

hence

$$f((xR_K)_S) = \prod_{v \in S_\infty} F_v(x^{-1}).$$

If $v(x-1)$ is small for Archimedean v, then $F_v(x)$ and $F_v(x^{-1})$ are both close to 1. Choosing for a given neighbourhood U of unity in G a suitable ϵ, we can ensure $f((xR_K)_S) \in U$ provided $v(x-1) < \epsilon$ holds for all $v \in S$. This establishes the sufficiency.

To prove the necessity let $f : G(K;S) \longrightarrow G$ be an admissible homomorphism. We have to define F so that for any idele $x = \langle x_v \rangle$, with $x_v = 1$ for $v \in S$, we have $F(x) = f \circ g(x)$, and moreover F is trivial on I_0 and continuous. Theorem 6.28 yields the existence of a sequence a_n of principal ideles such that

$$\lim_n v(x^{-1} - a_n) = 0 \tag{7.8}$$

holds for $v \in S$. Let I_n denote the ideal $g(a_n x)$ and put $J_n = (I_n)_S$. For arbitrary natural m, n we have

$$f(J_n)/f(J_m) = f((a_n a_m^{-1} R_K)_S),$$

and this tends to unity for m, n tending to infinity, since (7.8) implies

$$\lim_{m,n \to \infty} v(a_n a_m^{-1} - 1) = 0$$

for $v \in S$. Thus the sequence $f(J_n)$ converges to a limit, which is independent of the choice of a_n, because G is assumed to be complete. Now put $F(x) = \lim_n f(J_n)$. The resulting homomorphism of I_K into G is obviously trivial on I_0 (just put $a_n = x^{-1}$ for principal x) and now we have to check its continuity. Let U_1 be a given neighbourhood of the unit element of G. Take a positive ϵ such that for any principal idele $x = \langle x_v \rangle$ the inequalities $v(x_v - 1) < \epsilon$ for every $v \in S$ imply $f(g(x)) \in U_1$. Put $O_v = \{x_v : v(x_v - 1) < \epsilon\}$, and consider the following neighbourhood of unity in I_K:

$$U = \prod_{v \in S} O_v \times \prod_{v \notin S} U(K_v).$$

Any $x = \langle x_v \rangle$ in U satisfies $x_v \in U(K_v)$ for v outside S, thus

$$F(x) = \lim_n f((a_n R_K)_S). \tag{7.9}$$

For sufficiently large n we have $v(a_n - 1) < \epsilon$ for $v \in S$, which leads to $f((a_n R_K)_S) \in U_1$, and (7.9) shows now that $F(x)$ lies in the closure of U_1. Now let U_0 be any neighbourhood of unity in G, choose another neighbourhood U' of unity whose closure is contained in U_0, and apply the preceding argument. This gives the continuity of F.

Finally, we prove the uniqueness of F. Let S' be the complement of S, and for any idele x choose $a_n \in I_0$, satisfying (7.8). Then

$$F(x) = F(a_n x) = F(\xi_n)F(\eta_n),$$

where ξ_n and η_n are ideles whose components at $v \in S$ and $v \in S'$, respectively, agree with components of $a_n x$, whereas the remaining components are equal to 1. This implies

$$F(x) = \lim_n F(\xi_n)F(\eta_n) = \lim_n f(g(a_n x)),$$

because of $\xi_n \to 1$, and so F is determined by f. □

Corollary 1. *If S is a finite set of normalized valuations containing S_∞, and $f : G(K;S) \longrightarrow T$ is admissible, then the function $f_1 : G(K) \longrightarrow T$ defined by*

$$f_1(I) = \begin{cases} f(I) & \text{if } I \in G(K;S), \\ 0 & \text{otherwise,} \end{cases}$$

is a proper Hecke character. Conversely, every proper Hecke character can be obtained in this way.

Proof : If f is admissible, then Theorem 7.4 gives the existence of a character X of $C(K)$ satisfying $X(x) = f(g(x))$ for every idele $x = \langle x_v \rangle$ with $x_v = 1$ for $v \in S$. This shows that the components X_v of X are trivial on $U(K_v)$ for $v \notin S$, and it is clear that in this case f_1 coincides with the Hecke character induced by X and S. The converse is trivial. □

A large class of Hecke characters is induced by characters of the groups $H_I^*(K)$:

Corollary 2. *Let χ be a character of $H_I^*(K)$, let S be the set of all normalized valuations of K which are either Archimedean, or for which the prime ideal of R_v divides I, and let $\varphi : G(K;S) \longrightarrow H_I^*(K)$ be the canonical homomorphism. Then the function*

$$f(I) = \begin{cases} \chi(\varphi(I)) & \text{if } I \in G(K;S), \\ 0 & \text{otherwise,} \end{cases}$$

is a proper Hecke character, and the character X of $C(K)$ inducing f is of finite order.

Conversely, if X is a character of finite order of $C(K)$, then every Hecke character induced by X arises in this way from a character of $H_I^*(K)$ for a suitable ideal I.

Proof : Write $I = \prod_v \mathfrak{p}_v^{a_v}$ and consider the set A of all ideles $\langle x_v \rangle$ satisfying $v(x_v - 1) < 1/2$ for real Archimedean v, and $x_v \equiv 1 \pmod{\mathfrak{p}_v^{a_v}}$ for $\mathfrak{p}_v$ dividing I. Every principal idele $x \in A$ is totally positive and congruent to unity mod I, hence the principal ideal generated by x lies in the principal class

of $H_I^*(K)$, and so we get $\chi(\varphi((xR_K)_S)) = 1$, i.e., the composition $\chi \circ \varphi$ is admissible, and the preceding corollary shows that f is a proper Hecke character.

If X is the character of the idele class-group inducing f, then for any idele $x = \langle x_v \rangle$ in A, which additionally satisfies $v(x_v) = 1$ for $v \notin S$, we have $X(x) = f(g(a_n x)_S)$ for large n, with a_n as in (7.8), because the image of f is discrete. Since for v outside S the ideals $a_n x_v R_v$ and $a_n R_v$ coincide, we get $f(g(a_n x)_S) = f(g(a_n)_S)$. Finally we obtain $X(x) = 1$, because ultimately the a_n's fall into A. This proves the triviality of X on the subgroup $\overline{A}$ of $C(K)$, generated by the image of A. This subgroup has a non-void interior, hence is open, and by Corollary to Proposition 6.24 its index is finite. But then X must be of a finite order.

Now assume that X is a character of $C(K)$ having finite order. If $X = \prod_v X_v$, then each X_v is also of finite order. In particular we must have $X_v = 1$ for complex v, and either $X_v = 1$, or $X_v(x) = \operatorname{sgn}(x)$ for real v. If f is a Hecke character induced by X, and S is its exceptional set, then it suffices to show the existence of an ideal I such that if x is totally positive and $x \equiv 1 \pmod{I}$ holds, then $f((xR_K)_S) = 1$. But if for non-Archimedean v in S $\mathfrak{f}_v$ is the conductor of X_v, then the ideal

$$I = \prod_{v \in S \setminus S_\infty} \mathfrak{f}_v$$

satisfies our needs. □

Corollary 3. *If N is a positive rational integer, χ a character of the group $G(N) = (\mathbb{Z}/N\mathbb{Z})^*$, and X is the corresponding Dirichlet character, i.e.,*

$$X(n) = \begin{cases} \chi(|n| \bmod N) & \text{if } (n, N) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

then X is a proper Hecke character.

Proof : The group $G(N)$ is canonically isomorphic to $H_{N\mathbb{Z}}^*(\mathbb{Q})$ and we may apply Corollary 2. □

Later we shall have an opportunity to use the following result:

Corollary 4. *The canonical map $\varphi : G(K; S) \longrightarrow H_I^*(K)$, with S as in Corollary 2, is induced by a continuous homomorphism $F : C(K) \longrightarrow H_I^*(K)$, trivializing on the image of J_K'.*

Proof : The admissibility of φ is evident, and this provides the needed map F. Since J_K' is topologically isomorphic to the multiplicative group of positive reals it cannot have proper open subgroups, and so every continuous homomorphism into a finite group must necessarily be trivial. □

4. We shall establish now a relation between the system of all groups $H_I^*(K)$ and the factor-group $C(K)/D(K)$, where $D(K)$ is, as before, the connected component of the unit element of $C(K)$. This relation is of importance in the class-field theory, which provides a proof of the fact that the group $C(K)/D(K)$ is isomorphic to the Galois group of the maximal Abelian extension of K with the Krull topology, in which subgroups corresponding to finite extensions of K form a fundamental system of neighbourhoods of the unit element. Consider the inverse system consisting of all groups $H_I^*(K)$ with maps $t_{I,J} : H_I^*(K) \longrightarrow H_J^*(K)$ defined for all pairs I, J with $J|I$ in the following way: if $X \in H_I^*(K)$ then choose an ideal $A \in X$, and define $t_{I,J}(X)$ to be the class in $H_J^*(K)$ containing A. One sees easily that this definition does not depend on the particular choice of the ideal A. Denote by $H^{\#}(K)$ the inverse limit of this system.

Proposition 7.5. *(i) A character X of $C(K)$ induces a character of $H_I^*(K)$ for some I if and only if X is trivial on $D(K)$.*

(ii) The groups $H^{\#}(K)$ and $C(K)/D(K)$ are topologically isomorphic.

Proof : (i) Corollary 2 to Theorem 7.4 implies that if a character of the group $C(K)/D(K)$ induces a character of $H_I^*(K)$, then it must have a finite order, and the converse also holds. Therefore it remains to show that a character of $C(K)$ is of finite order if and only if it is trivial on $D(K)$, but this is easy. Indeed, if X is a character of $C(K)/D(K)$ of finite order, then it maps $D(K)$ onto a connected proper subgroup of T, i.e., $\{1\}$, and on the other hand, Corollary to Theorem 6.25 shows that the group $C(K)/D(K)$ is compact and totally disconnected, hence every its character is of finite order.

(ii) It follows from Theorem IV of Appendix I that the dual group H' of $H^{\#}(K)$ is the direct limit of the dual groups of $H_I^*(K)$. The map g, which maps every character X of $C(K)/D(K)$ onto an element of H', determined by the set of all characters of $H_I^*(K)$ induced by X, is a well-defined homomorphism. The uniqueness assertion of Theorem 7.4 jointly with Corollary 2 to that theorem shows that g is injective, and its surjectivity is a consequence of (i). The homomorphism g is trivially continuous since both groups are discrete, and it remains to apply the duality theorem. □

Now we define the *conductor* $\mathfrak{f} = \mathfrak{f}(\chi)$ of a Hecke character χ defined via a quasicharacter $X = \prod_v X_v$ of $C(K)$ with an exceptional set S. For $v \notin S_\infty$ let $\mathfrak{f}_v$ be the conductor of X_v, and put $\mathfrak{f} = \prod_v \mathfrak{f}_v$.

Proposition 7.6. *(i) If $x \in K^*$, then for the ideal $I = xR_K$ we have*

$$\chi(I) = \begin{cases} \prod_{v \in S} X_v(x^{-1}) & \text{if } I \text{ has no prime divisor } \mathfrak{p}_v \text{ with } v \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, if $x \equiv 1 \pmod{\mathfrak{f}}$, then

$$\chi(I) = \prod_{v \in S_\infty} X_v(x^{-1}).$$

(ii) If X is of finite order, $x \in K^*$ is totally positive and $x \equiv 1 \pmod{\mathfrak{f}}$, then $\chi(xR_K) = 1$. Moreover, if for an ideal $\mathfrak{f}_1$ the congruence $x \equiv 1 \pmod{\mathfrak{f}_1}$ implies $\chi(xR_K) = 1$ for totally positive x, then $\mathfrak{f} | \mathfrak{f}_1$.

Proof : (i) If I has a prime divisor $\mathfrak{p}_v$ with $v \in S$, then $\chi(I) = 0$. Otherwise, writing $I = \prod_{v \notin S} \mathfrak{p}_v^{\alpha_v}$ we get

$$\chi(I) = \prod_{v \notin S} X_v(\pi_v)^{\alpha_v},$$

where π_v is a generator of $\mathfrak{p}_v$. Since for $v \notin S$ the quasicharacter X_v is trivial on units, and for the image x_v of x in K_v one has $x_v = \epsilon_v \pi_v^{\alpha_v}$, thus $X_v(x_v) = X_v(\pi_v)^{\alpha_v}$. Since X is trivial on I_0, we have

$$1 = \prod_v X_v(x_v) = \chi(I) \prod_{v \in S} X_v(x_v),$$

and this gives the first equality.

To obtain the second observe that since $x \equiv 1 \pmod{\mathfrak{f}}$, we have $X_v(x) = 1$ for non-Archimedean $v \in S$, and so we may omit the factors corresponding to non-Archimedean v's.

(ii) Since X_v is of finite order, it equals either 1, or $\operatorname{sgn} x_v$ for Archimedean v's, hence for totally positive x the product $\prod_{v \in S_\infty} X_v(x^{-1})$ is equal to 1.

Now assume that $\mathfrak{f}_1 = \prod_v \mathfrak{p}_v^{n_v}$ is an ideal not dividing $\mathfrak{f}$, and having the property that for totally positive x satisfying $x \equiv 1 \pmod{\mathfrak{f}_1}$ we have $\chi(xR_K) = 1$. There exists v_0 such that $\mathfrak{f}_{v_0} = \mathfrak{p}_{v_0}^m$ holds with $m > n_v$, and therefore there is an element $a \in K_{v_0}^*$ with $X_{v_0}(a) \neq 1$, and a_{v_0} congruent to unity mod $\mathfrak{p}_{v_0}^{m-1}$. Choose a totally positive $x \in K^*$ with

$$\begin{aligned} x &\equiv a \pmod{\mathfrak{p}_{v_0}^{m-1}}, \\ x &\equiv 1 \pmod{\mathfrak{p}_v^{n_v}} \quad (v \neq v_0, \mathfrak{p}_v | \mathfrak{f}_1), \\ x &\equiv 1 \pmod{\mathfrak{f}_v} \quad (v \neq v_0, \mathfrak{p}_v \nmid \mathfrak{f}_1). \end{aligned}$$

Then $x \equiv 1 \pmod{\mathfrak{f}_1}$, hence $\chi(xR_K) = 1$. On the other hand

$$1 = X(x) = \chi^{-1}(I) \prod_{v \in S} X_v(x) = X_{v_0}(a_{v_0}) \neq 1,$$

a contradiction. □

It can be easily verified that in the case covered by Corollary 3 to Theorem 7.4 this definition of the conductor agrees with the usual one.

Our definition of Hecke characters does not formally agree with the classical one, due to Hecke, and we are now going to show that the two notions actually coincide. This is the content of the next proposition.

Proposition 7.7. *Let* $\mathfrak{f}$ *be a non-zero ideal of* R_K, *let* $\epsilon_1, \ldots, \epsilon_r$ *be a system of fundamental units of* $U^+(K, \mathfrak{f})$ *and let* ζ *be a generator of the group of all roots of unity contained in* K, *and congruent to unity* mod $\mathfrak{f}$. *For Archimedean* v *choose rational integers* n_v *satisfying*

$$\prod_{v \in S_\infty} F_v(\zeta)^{n_v} = 1, \tag{7.10}$$

and for each non-Archimedean v *choose a real number* a_v, *so that*

$$\sum_v a_v \log |F_v(\epsilon_j)| + \sum_{v \text{ complex}} n_v \arg F_v(\epsilon_j)$$

is an integral rational multiple of 2π *for* $j = 1, 2, \ldots, r$.

If the group $H^*_{\mathfrak{f}}(K)$ *has cyclic factors of orders* $h_1, \ldots, h_s$, *then choose ideals* $J_1, \ldots, J_s$ *whose classes generate these factors, and let* ψ *be an arbitrary character of* $H^*_{\mathfrak{f}}(K)$ *extended to a function defined on* $G(K)$. *For every totally positive* $x \in K^*$, *congruent to unity* mod $\mathfrak{f}$ *put*

$$f(x) = \prod_{v \in S_\infty} |x_v|^{ia_v} \prod_{v \text{ complex}} \left(\frac{x_v}{|x_v|} \right)^{n_v}, \tag{7.11}$$

and define for any ideal of the form $I = xJ_1^{b_1} \cdots J_s^{b_s}$ $(0 \leq b_i < h_i)$

$$\chi(I) = f(x) w_1^{b_1} \cdots w_s^{b_s} \psi(I), \tag{7.12}$$

where for $i = 1, 2, \ldots, s$ *the numbers* w_i *are arbitrarily fixed* h_i*-th roots of* $f(x_i)$, x_i *being a fixed generator of the principal ideal* $J_i^{h_i}$, *which is totally positive and congruent to unity* mod $\mathfrak{f}$.

The function χ *defined by* (7.12) *for ideals relatively prime to* $\mathfrak{f}$ *and by* $\chi(I) = 0$ *for the remaining ideals is a proper Hecke character. Conversely, every proper Hecke character is obtainable in this way.*

Proof : First we check that χ is well-defined, i.e., it depends only on I and not on the choice of x. It suffices to show that for every totally positive unit $\epsilon \equiv 1 \pmod{\mathfrak{f}}$ we have $f(\epsilon) = 1$. Of course, it is enough to do this for $\epsilon = \zeta, \epsilon_1, \ldots, \epsilon_r$.

Now, (7.10) implies $f(\zeta) = 1$ and from (7.11) we obtain

$$\log f(\epsilon_i) \equiv i \sum_{v \in S_\infty} a_v \log |F_v(\epsilon_i)| + \sum_{v \text{ complex}} n_v L_v(\epsilon_i) \pmod{2\pi i},$$

where $L_v(\epsilon_i) = \log(F_v(\epsilon_i)/|F_v(\epsilon_i)|)$. Our choice of the a_v's implies

$$\log f(\epsilon_i) \equiv 0 \pmod{2\pi i},$$

and so $f(\epsilon_i)$ is indeed equal to unity. Put $S = S_\infty \cup \{v : \mathfrak{p}_v | \mathfrak{f}\}$, and observe that χ is an admissible homomorphism of $G(K;S)$. This is accomplished by noting that if $v(x-1)$ is sufficiently small for $v \in S$, then x is totally positive, congruent to 1 mod $\mathfrak{f}$, and, for Archimedean v, x_v is close to 1. Thus $\chi(xR_K) = f(x)$ is by (7.11) close to unity. Now Corollary 1 to Theorem 7.4 shows that χ is indeed a Hecke character.

To prove the converse let χ be a Hecke character of conductor $\mathfrak{f}$. Take a totally positive element x of K^*, congruent to 1 mod $\mathfrak{f}$, and let $A = xR_K$. If now $X = \prod_v X_v$ is the character of the idele class-group inducing χ, then

$$X(\langle x_v \rangle) = \chi(g(\langle x_v \rangle_S)) \prod_{v \in S} X_v(x_v),$$

S being the exceptional set of χ. Since the value of X at the principal idele determined by x equals 1 we obtain

$$\chi(A) = \prod_{v \in S} X_v(x_v^{-1}).$$

The congruence $x \equiv 1 \,(\mathrm{mod}\, \mathfrak{f})$, and the total positivity of x shows that for non-Archimedean $v \in S$ we have $X_v(x_v) = 1$, and for $v \in S_\infty$ we have

$$X_v(x_v) = |x_v|^{ia_v} \left(\frac{x_v}{|x_v|}\right)^{n_v}$$

for some real a_v and rational integral n_v, equal to zero in the case of real v. Moreover, for $x = \zeta, \epsilon_1, \ldots, \epsilon_r$ we have $\chi(A) = 1$, and this leads to (7.10) and the asserted form of a_v. Thus, if $f(x)$ is the value of $\chi(A)$ in case of x totally positive and congruent to unity mod $\mathfrak{f}$, then it has the form given by (7.11). Now let $J_1, \ldots, J_s$, $x_1, \ldots, x_s$ be as in the theorem. If $I = xJ_1^{b_1} \cdots J_s^{b_s}$, with x totally positive and congruent to unity mod $\mathfrak{f}$, then $\chi(I) = f(x)\chi(J_1)^{b_1} \cdots \chi(J_s)^{b_s}$, and obviously $w_i = \chi(J_i)$ satisfies $w_i^{h_i} = f(x_i)$. It remains to observe that

$$\psi(I) = \frac{\chi(I)}{f(x) w_1^{b_1} \cdots w_s^{b_s}}$$

is a multiplicative function equal to unity on the set of all principal ideals having a generator which is totally positive, and congruent to unity mod $\mathfrak{f}$. But such function must necessarily be a character of $H_{\mathfrak{f}}^*(K)$, and so our proof is complete. □

5. Now we introduce zeta-functions associated with Hecke characters. As a special case we shall obtain the classical Dirichlet L-functions. For an arbitrary Hecke character χ we define the *Hecke zeta-function* by the formula

$$\zeta(s,\chi) = \sum_I \frac{\chi(I)}{N(I)^s},$$

the sum taken over all non-zero ideals of R_K.

Proposition 7.8. *If $\chi(I) = \chi_1(I)N(I)^w$ with a normalized Hecke character χ_1 and a complex w, then the series defining $\zeta(s,\chi)$ converges absolutely in the half-plane $\sigma > 1 + \mathrm{Re}\, w$, and defines there a regular function. Moreover in that half-plane we have*

$$\zeta(s,\chi) = \prod_{\mathfrak{p}} \left(\frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}\right),$$

and

$$\zeta(s,\chi) = \zeta(s-w,\chi_1).$$

Proof : It suffices to observe that the series for $\zeta(s,\chi)$ is majorized by the series for $\zeta_K(\mathrm{Re}\,(s-w))$, and to apply Proposition 7.2 and Lemma 7.1. □

This proposition shows that it suffices to study the behaviour of Hecke zeta-functions for normalized (hence proper) Hecke characters. This is accomplished in the following theorem:

Theorem 7.9. *Let X be a normalized character of $C(K)$ and let χ be the induced Hecke character with exceptional set S.*

(i) If $X = 1$, then

$$\zeta(s,\chi) = \zeta_K(s) \prod_{v\in S\setminus S_\infty} \left(1 - \frac{1}{N(\mathfrak{p}_v)^s}\right),$$

and so it is meromorphic with a simple pole at $s = 1$, where it has the residue

$$h\kappa \prod_{v\in S\setminus S_\infty} \left(1 - \frac{1}{N(\mathfrak{p}_v)}\right).$$

(ii) If $X \neq 1$, then $\zeta(s,\chi)$ can be analytically continued to an entire function satisfying the functional equation

$$\zeta(s,\chi) \prod_{v\notin S} N(D_v)^{-1/2} \prod_{v\in S} \rho_v(X_v v^s) = \zeta(1-s,\overline{\chi}) \prod_{v\notin S} (N(D_v)^{-s}\chi(D_v)),$$

where D_v is the different of the extension $K_v/\mathbb{Q}_p$, and ρ_v is the function defined on quasicharacters of K_v^* in Theorem 5.46 *and Appendix I.*

Proof : The assertion (i) results immediately from Theorem 7.3, and to prove (ii) we shall imitate the proof of that theorem. Consider the function $f(x) = \prod_v f_v(x_v)$, whose components f_v are defined in the following way:

If v is non-Archimedean and $\mathfrak{p}_v^{N_v}$ is the conductor of X_v the we put

$$f_v(x_v) = \begin{cases} \mathbf{X}(x_v) & \text{if } x_v \in (D_v \mathfrak{p}_v^{N_v})^{-1}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathbf{X}$ denotes the standard character of K_v^+. Note that this function occurred already in the proof of Theorem 5.46. First let v be real. If $X_v = v(x_v)^{it_v}$, then we put $f_v(x_v) = \exp(-\pi x_v^2)$, otherwise we put $f_v(x_v) = x_v \exp(-\pi x_v^2)$. If v is complex, and $X_v(x_v) = (x_v/|x_v|)^{N_v} v(x_v)^{it}$, then we put

$$f_v(x_v) = \begin{cases} \overline{x}_v^{N_v} \exp(-2\pi v(x_v)) & \text{if } N_v \geq 0, \\ x_v^{-N_v} \exp(-2\pi v(x_v)) & \text{if } N_v < 0. \end{cases}$$

These functions appear also in Appendix I in the proof of functional equations for zeta-functions in $\mathbb{R}$ and $\mathbb{C}$.

To check that f satisfies the assumptions of Theorem 6.36 we have to know the Fourier transforms $\hat{f}_v$. Luckily, they were computed in the proofs of Theorems 5.46, 7.3 and in the Appendix I, where the following results were obtained:

If $v \notin S$, then

$$\hat{f}_v(y_v) = \begin{cases} N(D_v)^{-1/2} & \text{if } y_v \in D_v^{-1}, \\ 0 & \text{otherwise,} \end{cases}$$

if $v \in S \setminus S_\infty$ and $N_v \neq 0$, then

$$\hat{f}_v(y_v) = \begin{cases} N(D_v)^{1/2} N(\mathfrak{p}_v)^{N_v} & \text{if } y_v \equiv 1 \pmod{\mathfrak{p}_v^{N_v}}, \\ 0 & \text{otherwise,} \end{cases}$$

if $v \in S \setminus S_\infty$ and $N_v = 0$, then

$$\hat{f}_v(y_v) = \begin{cases} N(D_v)^{1/2} & \text{if } y_v \in R_v, \\ 0 & \text{otherwise,} \end{cases}$$

and if $v \in S_\infty$, then

$$\hat{f}_v(y_v) = \begin{cases} f_v(y_v) & \text{if } v \text{ is real and } X_v = v^{it_v}, \\ i f_v(y_v) & \text{if } v \text{ is real and } X_v \neq v^{it_v}, , \\ i^{|N_v|} f_v(y_v) & \text{if } v \text{ is complex.} \end{cases}$$

Proceeding as in the proof of Theorem 7.3 we find that f indeed satisfies the assumptions of Theorem 6.36, and so we may apply it. Let

$$Z_v(f_v,s)=\int_{K_v^*} f_v(x_v)X_v(x_v)v(x_v)^s d\mu_v^*(x)$$

and let first $v\notin S$. Then, denoting by π_v a fixed generator of the ideal $\mathfrak{p}_v$, we get

$$\begin{aligned}Z_v(f_v,s)&=\int_{R_v} X_v(x_v)v(x_v)^s d\mu_v^*(x)=\sum_{j=0}^{\infty}\int_{\pi_v^j U(K_v)} X_v(x_v)^s d\mu_v^*(x)\\&=\sum_{j=0}^{\infty} X_v(\pi_v)^j N(\mathfrak{p}_v)^{-js}\int_{\pi_v^j U(K_v)} d\mu_v^*(x)\\&=\sum_{j=0}^{\infty} X_v(\pi_v)^j N(\mathfrak{p}_v)^{-js}\int_{U(K_v)} d\mu_v^*(x)\\&=N(D_v)^{-1/2}\sum_{j=0}^{\infty} X_v(\pi_v)^j N(\mathfrak{p}_v)^{-js},\end{aligned}$$

and so

$$Z_v(f_v,s)=N(D_v)^{-1/2}(1-\chi(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-s})^{-1} \tag{7.13}$$

holds for $v\notin S$.

Proceeding in the same way we obtain for

$$Z_v(\hat{f}_v,1-s)=\int_{K_v^*}\hat{f}_v(y_v)X_v(y_v)v(y_v)^{1-s}d\mu_v^*(y)$$

the following equalities

$$\begin{aligned}Z_v(\hat{f}_v,1-s)&=N(D_v)^{-1/2}\sum_{j=-m}^{\infty}\int_{\pi_v^j U(K_v)} X_v(y_v)^{1-s}d\mu_v^*(y)\\&=N(D_v)^{-1/2}\sum_{j=-m}^{\infty} N(\mathfrak{p}_v)^{-j(1-s)}X_v(\pi_v)^j\int_{U(K_v)} d\mu_v^*(y)\\&=N(D_v)^{-1}N(\mathfrak{p}_v)^{m(1-s)}X_v(\pi_v)^{-m}(1-X_v(\pi_v)N(\pi_v)^{s-1})^{-1},\end{aligned}$$

where we put $D_v=\mathfrak{p}_v^m$, and so

$$Z_v(\hat{f}_v,1-s)=N(D_v)^{-s}\chi(D_v)(1-\overline{\chi}(\pi_v)N(\mathfrak{p}_v)^{s-1})^{-1}. \tag{7.14}$$

For the zeta-function $Z(f,s)$ of f we obtain, in view of (7.13),

$$Z(f,s)=\prod_v Z_v(f_v,s)=\zeta(s,\chi)\prod_{v\notin S}N(D_v)^{-1/2}\prod_{v\in S}Z_v(f_v,s),$$

and, similarly, for the zeta-function $Z(\hat{f},1-s)$ (7.14) leads to

$$Z(\hat{f}, 1-s) = \prod_v Z_v(\hat{f}_v, 1-s)$$
$$= \zeta(1-s, \overline{\chi}) \prod_{v \notin S} N(D_v)^{-s} \chi(D_v) \prod_{v \in S} Z_v(\hat{f}_v, 1-s).$$

Now we may use Theorem 5.46 for non-Archimedean v, and Theorem VII of Appendix I for Archimedean v to obtain for $v \in S$

$$Z_v(f_v, s) = \rho_v(X_v v^s) Z_v(\hat{f}_v, 1-s),$$

and this together with the preceding two equalities proves the theorem. □

For later use we write now explicitly the zeta-function $Z(f, s)$ occurring in the proof of the last theorem:

Proposition 7.10. *If f is the function used in the proof of the theorem then*

$$Z(f, s) = \zeta(s, \chi) |d(K)|^{-1/2} P_1 P_2 P_3 P_4,$$

where

$$P_1 = \prod_{\substack{v \in S \\ \mathfrak{f}_v \neq 1}} \tau_0(X_v) N(\mathfrak{f}_v D_v)^s N(\mathfrak{f}_v)^{-1} (1 - N(\mathfrak{p}_v)^{-1})^{-1},$$

$$P_2 = \prod_{\substack{v \in S \\ \mathfrak{f}_v = 1}} N(D_v)^s (1 - N(\mathfrak{p}_v)^{-s})^{-1},$$

$$P_3 = \prod_{v \text{ real}} \Gamma\left(\frac{s + it_v + N_v}{2}\right) \pi^{-(s+it_v+N_v)/2},$$

and

$$P_4 = \prod_{v \text{ complex}} \Gamma\left(s + it_v + \frac{|N_v|}{2}\right) (2\pi)^{s+it_v-1-|N_v|)/2}.$$

Here $\mathfrak{f}_v$ denotes the conductor of X_v, and the numbers t_v and N_v are determined for $v \in S_\infty$ from

$$X_v(x_v) = \left(\frac{x_v}{|x_v|}\right)^{N_v} v(x_v)^{it_v},$$

with $N_v \in \mathbb{Z}$ for complex v, and $N_v \in \{0, 1\}$ for real v.

Proof : Combine the expressions for $Z_v(f_v, s)$ given in Proposition 5.45 and (7.13) for non-Archimedean v, and for v Archimedean use the results of Appendix I. □

6. Now we introduce primitive Hecke characters. This will enable us to put the results in a convenient form.

It is clear that the same quasicharacter of $C(K)$ defines several distinct Hecke characters with the help of distinct exceptional sets S. If S is chosen to be as small as possible, in which case it consists of all Archimedean valuations, and of those non-Archimedean v's for which X_v is non-trivial on the group of units, then the resulting character is called a *primitive Hecke character*. To every Hecke character there corresponds a unique primitive character induced by the same quasicharacter and having the smallest possible exceptional set. It is evident that for almost all prime ideals $\mathfrak{p}$ the $\mathfrak{p}$-parts of these two Hecke characters coincide.

We establish now the connection between this notion of primitivity and the usual notion of primitivity for Dirichlet characters. Note first that distinct Dirichlet characters, say χ_1, defined mod m and χ_2, defined mod n, may be used to define the same Hecke character $\chi(x\mathbb{Z})$ in the case when m and n have the same prime divisors and there is a number $r|(m,n)$, having the same prime divisors and a character χ_3, defined mod r such that

$$\chi_3(f_1(x)) = \chi_1(x), \quad \chi_3(f_2(y)) = \chi_2(y)$$

holds for $x \in G(m)$, $y \in G(n)$, with f_1, f_2 being the canonical homomorphisms of $G(m)$ and $G(n)$ onto $G(r)$. Clearly enough, this is the only case in which the equality of Hecke characters may arise.

Proposition 7.11. *If X is a primitive Hecke character induced by a Dirichlet character χ mod m, then there exists a primitive character ψ mod n, with a certain n dividing m, which also induces X. Conversely, every primitive Dirichlet character induces a primitive Hecke character.*

Proof : If χ mod m induces X, then the conductor of χ equals that of X, as was already observed after Proposition 7.7. If X_0 is the primitive character associated with X, and ψ is the primitive Dirichlet character associated with χ and having the conductor $n|m$, then ψ induces X_0. The converse is immediate. □

If χ, χ_1 are Hecke characters induced by the same quasicharacter of $C(K)$, χ_1 is primitive and S, S_1 are the corresponding exceptional sets, then

$$\zeta(s,\chi) = \zeta(s,\chi_1) \prod_{v \in S \setminus S_1} \left(1 - \frac{\chi(\mathfrak{p}_v)}{N(\mathfrak{p}_v)^s}\right), \tag{7.15}$$

and so the properties of $\zeta(s,\chi)$ may be obtained from the corresponding properties of $\zeta(s,\chi_1)$. This allows us to restrict our attention to primitive Hecke characters.

Now we can obtain the functional equation for the zeta-function of any primitive and normalized Hecke character χ. Denote by $\mathfrak{f}$ its conductor and let $X = \prod_v X_v$ be the character of $C(K)$ inducing χ. Let $\mathfrak{f}_v$ be the conductor of X_v for $v \notin S_\infty$, and for $v \in S_\infty$ write

$$X_v(x_v) = \left(\frac{x_v}{|x_v|}\right)^{N_v}, \quad N = \sum_v N_v, \quad T = \sum_{v \text{ complex}} t_v.$$

Proposition 7.12. *Under the above assumptions and notation we have the following functional equation for* $\zeta(s,\chi)$*:*

$$\begin{aligned}\zeta(s,\chi) i^{-N} \pi^{-n(s-1/2)} 2^{-2r_2(s-1/2)-2iT} |d(K)|^{s-1/2} N(\mathfrak{f})^{s-1} \\ \times \prod_{\mathfrak{p}_v | \mathfrak{f}} \tau_0(X_v) \prod_{v \text{ real}} \frac{\Gamma((N_v + s + it_v)/2)}{\Gamma((N_v + 1 - s - it_v)/2)} \\ \times \prod_{v \text{ complex}} \frac{\Gamma(|N_v|/2 + s + it_v)}{\Gamma(|N_v|/2 + 1 - s - it_v)} \\ = \prod_{v \notin S} \chi(D_v) \zeta(1-s, \overline{\chi}).\end{aligned}$$

Proof : Apply Theorem 7.9, using Theorem 5.46 and Theorem VII of Appendix I, which give an explicit form of ρ_v, remembering that for normalized characters we have $\sum_v t_v = 0$. □

Corollary. *If* χ *is a Hecke character induced by a character of some group* $H_{\mathfrak{f}}^*$ *of conductor* $\mathfrak{f}$*, then for its zeta-function we have*

$$\begin{aligned}\zeta(s,\chi) i^{-N} \pi^{-n(s-1/2)} 2^{-2r_2(s-1/2)} |d(K)|^{s-1/2} N(\mathfrak{f})^{s-1} \\ \times \prod_{\mathfrak{p}_v | \mathfrak{f}} \tau_0(X_v) \left(\frac{\Gamma(s/2)}{\Gamma((1-s)/2)}\right)^B \\ \times \left(\frac{\Gamma((1+s)/2)}{\Gamma((2-s)/2)}\right)^{r_1 - B} \left(\frac{\Gamma(s)}{\Gamma(1-s}\right)^{r_2} \\ = \zeta(1-s, \overline{\chi}) \prod_{\mathfrak{p}_v \nmid \mathfrak{f}} \chi(D_v),\end{aligned}$$

B being the number of real v*'s with* $X_v = 1$.

Proof : Since by Corollary 2 to Theorem 7.4 the characters X_v are of finite order, we can apply the last Proposition with $t_v = 0$ for all v's and $N_v = 0$ for complex v's. □

Sometimes the following, slightly less precise, form of the functional equation is sufficient for applications:

Corollary 1. *Under the assumptions of the proposition 7.12 one has*

$$\begin{aligned}\zeta(s,\chi) =& W(\chi)\zeta(1-s,\overline{\chi})\pi^{n(s-1/2)}2^{2r_2(s-1/2)} \\ &\times (N(\mathfrak{f})|d(K)|)^{1/2-s}\prod_{v \text{ real}}\frac{\Gamma((N_v+1-s-it_v)/2)}{\Gamma((N_v+s+it_v)/2)} \\ &\times \prod_{v \text{ complex}}\frac{\Gamma(|N_v|/2+1-s-it_v)}{\Gamma(|N_v|/2+s+it_v)}, \qquad (7.16)\end{aligned}$$

where $|W(\chi)| = 1$.

Proof : To prove this equality apply the preceding proposition, remembering that by Proposition 5.47 (iii) the product

$$\prod_{\mathfrak{p}_v|\mathfrak{f}}\tau_0(X_v)$$

is of absolute value $\sqrt{N(\mathfrak{f})}$. □

Corollary 2. *Let f be a primitive Dirichlet character* mod N *and let χ be the corresponding Hecke character. Assume $N > 1$ and write $N = \prod_{i=1}^{r} p_i^{a_i}$ with all a_i's positive. Then the function defined for $\sigma > 1$ by*

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

extends to an integral function, satisfying the functional equation

$$L(s,\chi)N^{s-1/2}\Gamma(s/2)\pi^{-s/2} = W(\chi)L(1-s,\overline{\chi})\Gamma((1-s)/2)\pi^{(s-1)/2},$$

if f is even, i.e., $f(-1) = 1$, and

$$L(s,\chi)N^{s-1/2}\Gamma((1+s)/2)\pi^{-(1+s)/2} = W(\chi)L(1-s,\overline{\chi})\Gamma((2-s)/2)\pi^{(s-2)/2},$$

if f is odd. Here $W(\chi)$ is a complex number of absolute value 1. □

7. Now we work out some evaluations of zeta-functions, which will find applications in subsequent sections.

Theorem 7.13. *Let χ be a normalized primitive Hecke character induced by a character of $H_{\mathfrak{f}}^*$, where $\mathfrak{f}$ is the conductor of χ. Write $D = |d(K)|N(\mathfrak{f})$ and let $a < 0$ and $b = 1-a$ be real numbers. Then in the region $a \le \sigma \le b$, $|t| \ge 2$ one has*

$$|\zeta(s,\chi)| \ll |t|^{(1/2-a)n},$$

with $n = [K:\mathbb{Q}]$, and the implied constant depending on a and $\mathfrak{f}$.

Proof : A lemma is needed first.

Lemma 7.14. *Under the assumptions of the theorem we have in every fixed region $c_1 \le \sigma \le c_2$, $|t| \ge c_3 > 0$ the equality*

$$\zeta(s,\chi) = W_1(\chi)\zeta(1-s,\overline{\chi})N(\mathfrak{f})^{1/2-s}\frac{\zeta_K(s)}{\zeta_K(1-s)}(1+O(\exp(-c_4|t|)),$$

with $c_4 > 0$ and $|W_1(\chi)| = 1$. The implied constant depends only on c_1, c_2 and c_3.

Proof : Equality (7.16) implies in our case

$$\begin{aligned}\frac{\zeta(s,\chi)}{\zeta(1-s,\overline{\chi})} &= W(\chi)\pi^{\alpha}2^{\beta}D^{1/2-s}\left(\frac{\Gamma((1-s)/2)}{\Gamma(s/2)}\right)^{B} \\ &\quad\times\left(\frac{\Gamma((2-s)/2)}{\Gamma((1+s)/2)}\right)^{r_1-B}\left(\frac{\Gamma(1-s)}{\Gamma(s)}\right)^{r_2} \\ &= W(\chi)N(\mathfrak{f})^{1/2-s}\left(\frac{\Gamma((2-s)/2)\Gamma(s/2)}{\Gamma((1-s)/2)\Gamma((1+s)/2)}\right)^{r_1-B} \\ &\quad\times\frac{\zeta_K(s)}{\zeta_K(1-s)},\end{aligned}$$

where $\alpha = n(s-1/2)$, $\beta = 2r_2(s-1/2)$, and B is as in the Corollary to Proposition 7.12.

But $\Gamma(z)\Gamma(1-z) = \pi/\sin(\pi z)$, and so we get

$$\begin{aligned}\frac{\Gamma((2-s)/2)\Gamma(s/2)}{\Gamma((1-s)/2)\Gamma((1+s)/2)} &= \frac{\cos(\pi s/2)}{\sin(\pi s/2)} \\ = i\frac{\exp(\pi si/2)+\exp(-\pi si/2)}{\exp(\pi si/2)-\exp(-\pi si/2)} &= -i\frac{1+\exp(\pi si)}{1-\exp(\pi si)} \\ &= -i+O(\exp(-\pi|t|)),\end{aligned}$$

proving the lemma. □

To deduce the theorem consider the function

$$f(s) = \zeta(s,\chi)s^{n(a-1/2)}$$

in the region $\{s:\ a \le \sigma \le b, |t| \ge 2\}$. Our aim is to show that f is bounded in that region, and to do this we use the Phragmén-Lindelöf theorem, applying it to both components of our region. It clearly suffices to consider only s in $\Xi = \{s:\ a \le \sigma \le b, t \ge 2\}$, since the general case will follow if we replace our zeta-function by the zeta-function attached to $\overline{\chi}$. So we have to prove first

$$|f(s)| \ll \exp(ct) \tag{7.17}$$

for a certain c and all $s \in \Xi$, and then

$$|f(s)| \ll 1 \tag{7.18}$$

for $s = a + it$ and $s = b + it$ $(t \geq 2)$.

To obtain (7.17) note that Proposition 7.10 and the last part of Theorem 6.36 imply the following evaluation, holding for all s in Ξ:

$$|\zeta(s,\chi)| \ll \sqrt{|d(K)|}N(\mathfrak{f})^{1/2-\sigma} \prod_{\mathfrak{p}_v|\mathfrak{f}} N(D_v)^{-\sigma}(1 - N(\mathfrak{p}_v)^{-1})$$
$$\times\ \pi^m 2^{m_1} |\Gamma(s/2)^{-B}\Gamma((1+s)/2)^{B-r_1}\Gamma(s)^{-r_2},$$

where $m = \sigma B/2 + (1+\sigma)(r_1 - B)/2 + (\sigma - 1)r_2$ and $m_1 = (\sigma - 1)r_2$. One has only to remember that all functions

$$|\Gamma(s)|^{-1},\ |\Gamma((1-s)/2)|^{-1},\ |\Gamma((2-s)/2)|^{-1}$$

are $O(\exp(ct))$ with some $c > 0$. Indeed, more precise evaluations of the gamma-function are provided by

$$|t|^{\sigma-1/2}\exp(-\pi|t|/2) \ll |\Gamma(s)| \ll |t|^{\sigma-1/2}\exp(-\pi|t|/2). \tag{7.19}$$

They will be useful in the proof of (7.18).

For $s = b + it$ we get, by Corollary 3 to Proposition 7.2, the bound

$$|\zeta(s,\chi)| = |\sum_I \frac{\chi(I)}{N(I)^s}| \leq \zeta_K(b) \leq \zeta_{\mathbb{Q}}(b).$$

In view of $|s|^{n(a-1/2)} \ll 1$ this gives $f(s) = O(1)$ on the line $\sigma = b$.

To obtain the same assertion for $\sigma = a$ write, using Lemma 7.14,

$$\zeta(a+it,\chi)$$
$$= W_1(\chi)\zeta(b-it,\overline{\chi})N(\mathfrak{f})^{1/2-a-it}\frac{\zeta_K(a+it)}{\zeta_K(b-it)}(1 + O(\exp(-c_4 t))),$$

and apply Theorem 7.3 (and its notation) to get

$$\frac{\zeta_K(a+it)}{\zeta_K(b-it)} = A^{1-2(a+it)}\left(\frac{\Gamma((b-it)/2)}{\Gamma((a+it)/2)}\right)^{r_1}\left(\frac{\Gamma(b-it)}{\Gamma(a+it)}\right)^{r_2}.$$

This leads, in view of (7.19) to

$$|\zeta(a+it,\chi)| \ll |t|^{(1/2-a)n}$$

and the bound (7.18) follows. By the theorem of Phragmén-Lindelöf the function f is bounded throughout Ξ. □

8. We conclude this section with the proof of a result concerning the zeros of $\zeta(s,\chi)$, which will be very useful in the next section, dealing with the distribution of prime ideals.

Theorem 7.15. *If $\chi(I) = \chi_1(I)N(I)^w$ is an arbitrary Hecke character, and χ_1 is the corresponding normalized character, then the zeta-function $\zeta(s,\chi)$ does not vanish in the closed half-plane $\sigma \geq 1 + \operatorname{Re} w$. In particular, if χ is proper (i.e., $\operatorname{Re} w = 0$), then $\zeta(s,\chi) \neq 0$ for $\sigma \geq 1$.*

Proof : By Proposition 7.8 we may assume that χ is normalized, i.e. $w = 0$. For $\sigma > 1$ the assertion follows from the non-vanishing of the Euler product of our zeta-function. So let us assume that $1+it$ is a zero of $\zeta(s,\chi)$, and exclude for the moment the case, when $t = 0$ and χ is a real character. Denote by χ_0 the character with the same exceptional set S as χ, generated by the trivial character of $C(K)$. In the open half-plane $\sigma > 1$ we may write

$$\zeta(s,\chi_0) = \exp\left(\sum_{v\notin S}\sum_{j=1}^{\infty} j^{-1}N(\mathfrak{p}_v)^{-js}\right),$$

$$\zeta(s,\chi) = \exp\left(\sum_{v\notin S}\sum_{j=1}^{\infty} j^{-1}\chi(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-js}\right),$$

and

$$\zeta(s,\chi^2) = \exp\left(\sum_{v\notin S}\sum_{j=1}^{\infty} j^{-1}\chi^2(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-js}\right).$$

Now, the series

$$\sum_{v\notin S}\sum_{j=2}^{\infty} j^{-1}f(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-js}$$

with f equal to 1, χ, or χ^2 is absolutely and uniformly convergent in the closed half-plane $\sigma \geq 1/2+\epsilon$ for every fixed positive ϵ, and so it defines there a regular function. Indeed, it is majorized by

$$\sum_{\mathfrak{p}}\sum_{j=2}^{\infty} N(\mathfrak{p})^{-j\sigma} = \sum_{\mathfrak{p}}\left(N(\mathfrak{p})^{2\sigma} - N(\mathfrak{p})^{\sigma}\right)^{-1}$$
$$\leq [K:\mathbb{Q}]\sum_{p}(p^{2\sigma} - p^{\sigma})^{-1},$$

and the last series is evidently convergent uniformly in $\sigma \geq 1/2+\epsilon$. We can thus write

$$\begin{aligned}\zeta(s,\chi_0) &= H_0(s)g_0(s),\\ \zeta(s,\chi) &= H_1(s)g_1(s),\\ \zeta(s,\chi^2) &= H_2(s)g_2(s),\end{aligned}$$

where g_0, g_1, g_2 are regular and non-vanishing in the open half-plane $\sigma > 1/2$ and

$$H_i(s) = \exp\left(\sum_{v \notin S} f_i(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-s}\right),$$

where $f_0 = \chi_0$, $f_1 = \chi$ and $f_2 = \chi^2$.

Let $1 + it_0$ be a zero of $\zeta(s, \chi)$ with $t \neq 0$ and consider the function $F(\sigma) = H_0^3(\sigma) H_1^4(\sigma + it_0) H_2(\sigma + 2it_0)$. We assert

$$\lim_{\sigma \to 1} F(\sigma + it_0) = 0. \tag{7.20}$$

Indeed, $H_1(1+it_0) = 0$ implies that $H_1(\sigma+it_0)/(\sigma-1)$ tends to a finite limit, say a, as σ approaches 1. Theorem 7.9 (i) shows that $H_0(s)$ has a simple pole at $s = 1$, and so $H_0(\sigma)(\sigma - 1)$ tends to a finite limit, say b, when σ tends to 1. Finally $H_2(s)$ is regular at $s = 1 + 2it_0$, because otherwise we would have $\chi^2 = \chi_0$ and $t = 0$, the case which we excluded for the time being. But

$$F(\sigma + it_0) = H_0^3(\sigma)(\sigma - 1)^3 H_1^4(\sigma + it_0)(\sigma - 1)^4 H_2(\sigma + 2it_0)(\sigma - 1),$$

and therefore

$$\lim_{\sigma \to 1} F(\sigma + it_0) = a^3 b^4 H_2(1 + 2it_0) \lim_{\sigma \to 1} (\sigma - 1) = 0,$$

settling (7.20). On the other hand, we have

$$F(\sigma + it_0) = \exp\left(\sum_{v \notin S} \frac{1}{N(\mathfrak{p}_v)^\sigma} (3 + 4\chi(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-it_0} + \chi^2(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-2it_0})\right),$$

and the absolute value of the last expression equals

$$\exp\left(\sum_{v \notin S} \frac{1}{N(\mathfrak{p}_v)^\sigma} (3 + 4\mathrm{Re}\ (\chi(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-it_0}) + \mathrm{Re}\ (\chi^2(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-2it_0}))\right).$$

Putting $\cos\theta_v = \mathrm{Re}\ (\chi(\mathfrak{p}_v) N(\mathfrak{p}_v)^{-it_0}$, we obtain

$$\begin{aligned} |F(\sigma + it_0)| &= \exp\left(\sum_{v \notin S} \frac{3 + 4\cos\theta_v + \cos 2\theta_v}{N(\mathfrak{p}_v)^\sigma}\right) \\ &= \exp\left(2 \sum_{v \notin S} \frac{(1 + \cos\theta_v)^2}{N(\mathfrak{p}_v)^\sigma}\right) \geq 1, \end{aligned}$$

contradicting (7.20).

It remains to prove our theorem in the case when χ is real and $t_0 = 0$. Of course, only the case $\chi \neq \chi_0$ is of interest, since $\zeta(s, \chi_0)$ has a pole at $s = 1$. Assume thus $\chi \neq \chi_0$ and $\zeta(1, \chi) = 0$. In this case we can write for $\sigma > 1$

$$\zeta(s,\chi)\zeta(s,\chi_0) = \exp G(\chi,s),$$

where

$$G(\chi,s) = \sum_{v\notin S}\sum_{j=1}^{\infty}\frac{1}{j}\frac{1+\chi(\mathfrak{p}_v)^j}{N(\mathfrak{p}_v)^{sj}}.$$

The assumption $\chi^2 = \chi_0$ shows that χ assumes only the values 0, 1 and -1, and thus $1+\chi(\mathfrak{p}_v)^j \geq 0$. Moreover, if $s > 1/2$ then for every fixed T we have

$$\sum_{\substack{v\notin S\\ N(\mathfrak{p}_v)\leq T}}\sum_{j=1}^{\infty}\frac{1}{j}\frac{1+\chi(\mathfrak{p}_v)^j}{N(\mathfrak{p}_v)^{sj}} \geq \frac{1}{2}\sum_{\substack{v\notin S\\ N(\mathfrak{p}_v)\leq T}}\frac{1}{N(\mathfrak{p}_v)^{2s}},$$

and with a suitable choice of T and $s > 1/2$ we can make the right-hand side arbitrarily large by Proposition 7.2 and Theorem 7.3. This shows that the series defining $G(\chi,s)$ cannot converge at $s = 1/2$. Observe now that this series is a Dirichlet series with non-negative coefficients, and so Theorem II of Appendix II shows that $G(\chi,s)$ must have a singularity on the real interval $[1/2,1]$. Since $G(\chi,s)$ is non-negative on this interval, the function $\exp G(\chi,s)$ must also have there a singularity. The only possible point where this may happen is $s = 1$, but $\zeta(s,\chi_0)$ has a simple pole there, and $\zeta(s,\chi)$ has a zero, implying that $\exp G(\chi,s)$ is regular at $s = 1$, which gives a contradiction. □

Corollary. *Dedekind's zeta-function ζ_K and Dirichlet's L-functions do not vanish on the line $\sigma = 1$.* □

7.2. Asymptotic Distribution of Ideals and Prime Ideals

1. We are now going to apply the analytical results obtained in the preceding section to the problem of distribution of ideals and prime ideals. We shall also use various results concerning Dirichlet series, including a Tauberian theorem of Ikehara-Delange, an account of which may be found in Appendix II, and also the method of complex integration.

To avoid endless repetitions we adopt the following convention in the sequel: as in the preceding chapter we shall write the complex variable s in the form $s = \sigma + it$, by $g(s)$ (with, or without indices) we shall denote functions regular in the closed half-plane $\sigma > 1$, not always the same even in the same chain of formulas. (So we will write, for example, $x^s + 1/s = x^s + g(s) = g(s)$.) If S a subset of the set of all normalized valuations of an algebraic number field K, then we shall write $\mathfrak{p} \in S$, to mean $\mathfrak{p} = \mathfrak{p}_v$, $v \in S$. If A is a set of prime ideals and for $\sigma > 1$ we have

$$\sum_{\mathfrak{p}\in A}\frac{1}{N(\mathfrak{p})^s} = a\log\frac{1}{s-1} + g(s)$$

with a certain real a, then we say that A is a *regular set of prime ideals*, and call a its *Dirichlet density*. Sometimes it is convenient to speak about the Dirichlet density of non-regular sets as well. We shall say that such set A has density a if the quotient

$$\left(\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-s}\right) : \left(a \log \frac{1}{s-1}\right)$$

tends to unity as $s > 1$ approaches 1 through real values. The existence of important regular sets will be demonstrated later on. Finally, the symbols $\sum_I$, $\sum_{\mathfrak{p}}$ will denote sums taken over all non-zero ideals, and non-zero prime ideals of R_K, respectively. The letter $\mathfrak{p}$ will always denote a prime ideal.

Almost everything which follows is based on the following assertion:

Proposition 7.16. *If χ is a normalized Hecke character, and S is its exceptional set, then for $\sigma > 1$ we have*

$$\zeta(s,\chi) = \sum_I \chi(I)N(I)^{-s} = \frac{\alpha(\chi)}{s-1} + g(s),$$

and

$$\sum_{\mathfrak{p}} \chi(\mathfrak{p})N(\mathfrak{p})^{-s} = \beta(\chi)\log\frac{1}{s-1} + g(s),$$

where

$$\alpha(\chi) = h\kappa \prod_{\mathfrak{p}\in S}\left(1 - \frac{1}{N(\mathfrak{p})}\right), \quad \beta(\chi) = 1,$$

if χ is the trivial character, and

$$\alpha(\chi) = \beta(\chi) = 0$$

otherwise.

Proof : The first equality is an immediate consequence of Theorem 7.9, since in view of Theorem 7.3 the residue of $\zeta_K(s)$ at $s = 1$ equals $h\kappa$. To prove the second equality write for $\sigma > 1$

$$\zeta(s,\chi) = G(s)\exp\left(\sum_{\mathfrak{p}\notin S}\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s)}\right),$$

where

$$G(s) = \exp\left(\sum_{\mathfrak{p}\notin S}\sum_{j=2}^{\infty}\frac{1}{j}\frac{\chi(\mathfrak{p})^j}{N(\mathfrak{p})^{js}}\right)$$

is regular and non-vanishing for $\sigma > 1/2$. This leads to

$$\sum_{\mathfrak{p}} \chi(\mathfrak{p}) N(\mathfrak{p})^{-s} = \log \zeta(s, \chi) - \log G(s) = \log \zeta(s, \chi) + g(s),$$

and the right-hand side of this equality is, by Theorem 7.15, regular for $\sigma \geq 1$, with the exception of $s = 1$ in the case of trivial χ. In this exceptional case we have, by Theorems 7.9 and 7.15, the equality

$$\zeta(s, \chi) = \frac{g(s)}{s-1},$$

with $g(s)$ not vanishing on the line $\sigma = 1$. Taking logarithms we arrive at the second asserted equality. □

Corollary 1. *The set of all prime ideals of R_K is regular, and its Dirichlet density equals* 1. □

Corollary 2. *The set A of all prime ideals of R_K having degree* 1 *over $\mathbb{Q}$ is regular, and its Dirichlet density equals* 1.

Proof : For $\sigma > 1$ we have

$$\sum_{\mathfrak{p} \in A} \frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} - \sum_{\mathfrak{p} \notin A} \frac{1}{N(\mathfrak{p})^s},$$

and the series $\sum_{\mathfrak{p} \notin A} N(\mathfrak{p})^{-s}$ is majorized by

$$[K : \mathbb{Q}] \sum_{p} \sum_{k=2}^{\infty} \frac{1}{p^{k\sigma}},$$

converging uniformly in the half-plane $\sigma \geq 3/4$, and so the proposition implies

$$\sum_{\mathfrak{p} \in A} \frac{1}{N(\mathfrak{p})^s} = \log \frac{1}{s-1} + g(s). \qquad \square$$

Corollary 3. *If L/K is a finite extension, and A is the set of all prime ideals of R_L of degree* 1 *over K, then A is regular, and its Dirichlet density equals* 1.

Proof : Let B be the set of all prime ideals of R_L of degree 1 over $\mathbb{Q}$. Clearly $B \subset A$, and

$$\sum_{\mathfrak{p} \in A \setminus B} \frac{1}{N(\mathfrak{p})^s} = g(s),$$

this series being a subseries of $\sum_{\mathfrak{p} \notin B} N(\mathfrak{p})^{-s}$, which, as we have just seen, converges uniformly for Re $s \geq 3/4$. Hence, using Corollary 2, we obtain our assertion. □

The next corollary provides another proof of Theorem 4.37:

Corollary 4. *Let L/K be a normal extension of degree N, and let A be the set of all prime ideals of R_K which split in L/K, i.e., which become products of N distinct prime ideals of the first degree in L. Then A is regular and its Dirichlet density is $1/N$.*

Proof : Since L/K is normal, a prime ideal of R_K splits in L/K if and only if it has at least one unramified prime divisor of first degree in L. Hence

$$\sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{N} \sum_{\mathfrak{P}}^{*} \frac{1}{N(\mathfrak{P})^s},$$

the sum $\sum^*$ taken over all unramified prime ideals of R_K with $f_{L/K}(\mathfrak{P}) = 1$. Since the number of ramified prime ideals is finite, the preceding corollary gives

$$\sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{N} \log \frac{1}{s-1} + g(s). \qquad \square$$

Corollary 5. *If L/K is of degree $N \geq 2$, then there exist infinitely many prime ideals of R_K which do not split in L/K. If, moreover, L/K is normal, then such ideals form a regular set of Dirichlet density $1 - 1/N$.*

Proof : If L/K is normal, then the assertion follows from Corollaries 1 and 4. If L/K is not normal, and $L = L_1, \ldots, L_r$ are all conjugates of L over K, then their composite field M is normal over K. If $\mathfrak{p}$ splits in L/K. then by Corollary to Theorem 5.11 it splits also in M/K, hence we may apply the part already proved. $\square$

It should be noted that one cannot replace the words "do not split" in the last corollary by "remain prime", even in the case $K = \mathbb{Q}$. Indeed, if $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_8)$, then Theorem 4.40 shows that if an odd prime would generate a prime ideal of R_L, then it would be a primitive root mod 8, but there are no such primitive roots at all, and the prime 2 does not remain prime already in $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$. Later we shall prove (see Corollary 2 to Theorem 7.29) that a similar situation arises for every normal non-cyclic extension.

Corollary 6. *If I is a non-zero ideal of R_K and $X \in H_I^*(K)$, then the set of all prime ideals lying in X is regular, and has $1/h_I^*(K)$ for its density.*

Proof : Let $\mathcal{X}$ be the set of all characters of $G_I^*(K)$. By the orthogonality of characters in finite Abelian groups we obtain for $\sigma > 1$ the equality

$$\sum_{\mathfrak{p}\in X} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{h_I^*(K)} \sum_{\chi\in\mathcal{X}} \overline{\chi}(X) \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Since every character of $H_I^*(K)$ can be considered as a Hecke character, Proposition 7.16 implies our assertion. □

Corollary 7. *In every class of $H_I^*(K)$ there are infinitely many prime ideals of the first degree.*

Proof : Apply Corollary 6 and note that by Corollary 2 every set of prime ideals of degree ≥ 2 is regular and has density zero. □

Note that in the special case $K = \mathbb{Q}$ the last corollary coincides with Dirichlet's prime number theorem in its qualitative form.

2. Now we turn to quantitative results.

Proposition 7.17. *(i) If χ is a normalized Hecke character, then*

$$\sum_{N(I)\leq x} \chi(I) = (\alpha(\chi) + o(1))x,$$

and

$$\sum_{N(\mathfrak{p})\leq x} \chi(\mathfrak{p}) = (\beta(\chi) + o(1))\frac{x}{\log x},$$

where $\alpha(\chi)$ and $\beta(\chi)$ are defined in Proposition 7.16.

(ii) If A is a regular set of prime ideals, c is its density and

$$A(x) = \sum_{\substack{\mathfrak{p}\in A \\ N(\mathfrak{p})\leq x}} 1,$$

then

$$A(x) = (c + o(1))\frac{x}{\log x}.$$

Proof : Part (i) in the case of trivial χ, and part (ii) in the case $c \neq 0$ result immediately from Theorem I of Appendix II and Proposition 7.16.

If the character χ is non-trivial, put

$$a_m = \sum_{N(I)=m} 1, \quad b_m = 2a_m + \sum_{N(I)=m} (\chi(I) + \overline{\chi}(I)) \geq 0.$$

Proposition 7.16 shows that for $\sigma > 1$ we have

$$\sum_{m=1}^{\infty} \frac{b_m}{m^s} = 2\zeta_K(s) + \zeta(s,\chi) + \zeta(s,\overline{\chi}) = \frac{2h\kappa}{s-1} + g(s),$$

and so Theorem I of Appendix II implies

$$\sum_{m \le x} b_m = (2h\kappa + o(1))x.$$

The same theorem implies also

$$2\sum_{m \le x} a_m = (2h\kappa + o(1))x,$$

thus

$$\sum_{N(I) \le x} (\chi(I) + \overline{\chi}(I)) = o(x),$$

leading to

$$\operatorname{Re}\left(\sum_{N(I) \le x} \chi(I)\right) = o(x).$$

Considering the sequence

$$c_m = 2a_m - i \sum_{N(I) \le x} (\chi(I) - \overline{\chi}(I))$$

we obtain in the same way

$$\operatorname{Im} \sum_{N(I) \le x} \chi(I) = o(x),$$

and the first assertion of (i) follows. The second follows by the same argument, in which $\zeta_K(s)$ is replaced by $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$.

Finally, to prove (ii) in the case $c = 0$ observe that Corollary 4 to Proposition 7.16 implies that for every $\epsilon > 0$ there exists a regular set of prime ideals A_ϵ with a positive density smaller that ϵ. Applying (ii) (already proved for $c > 0$) to the set $A \cup A_\epsilon$ we get

$$A(x) \le (\epsilon + o(1)\frac{x}{\log x},$$

i.e.,

$$\limsup_{x \to \infty} \frac{A(x) \log x}{x} \le \epsilon,$$

and since ϵ may be arbitrarily small, we get our assertion. □

Corollary 1. (The Prime Ideal Theorem). *If $\pi_K(x)$ denotes the number of prime ideals of R_K with norms not exceeding x, then*

$$\pi_K(x) = (1 + o(1))\frac{x}{\log x}. \qquad \square$$

Corollary 2. *If $\pi'_K(x)$ denotes the number of prime ideals of R_K of first degree with norms not exceeding x, then*

$$\pi'_K(x) = (1 + o(1))\frac{x}{\log x}. \qquad \square$$

Corollary 3. *If L/K is a normal extension of degree N, and $A_{L/K}(x)$ denotes the number of prime ideals of R_K splitting in L/K, and having norms not exceeding x, then*

$$A_{L/K}(x) = \left(\frac{1}{N} + o(1)\right)\frac{x}{\log x}. \qquad \square$$

Corollary 4. (The Prime Ideal Theorem for ideal classes). *If X is a class in $H_I^*(K)$, and $\pi_X(x)$ denotes the number of prime ideals in X with norms not exceeding x, then*

$$\pi_X(x) = \left(\frac{1}{h_I^*(K)} + o(1)\right)\frac{x}{\log x}. \qquad \square$$

(For $K = \mathbb{Q}$ this gives the quantitative form of Dirichlet's prime number theorem in its weak form, i.e., without any evaluation of the error term.)

Our next results concern the number of ideals with bounded norms.

Theorem 7.18. *If I is an ideal in R_K, X is a class of $H_I^*(K)$, and $M_X(x)$ is the number of ideals in X with norms not exceeding x, then*

$$M_X(s) = \left(\frac{\varphi(I)h\kappa}{N(I)h_I^*(K)} + o(1)\right)x.$$

Proof : We proceed in the same manner as in the proof of Corollary 6 to Proposition 7.16 and write $\mathcal{X}$ for the set of all characters of $H_I^*(K)$. If $F_X(m)$ is the number of ideals of X with norm m, then for $\sigma > 1$ we get by Proposition 7.16 the equality

$$\begin{aligned}\sum_{m=1}^{\infty}\frac{F_X(m)}{m^s} &= \sum_{I\in X}\frac{1}{N(I)^s} = \frac{1}{h_I^*(K)}\sum_{\chi\in\mathcal{X}}\overline{\chi}(X)\zeta(s,\chi)\\ &= \frac{h\kappa}{h_I^*(K)}\prod_{\mathfrak{p}|I}\left(1-\frac{1}{N(\mathfrak{p})}\right)\frac{1}{s-1} + g(s)\\ &= \frac{h\kappa\varphi(I)}{h_I^*(K)N(I)}\frac{1}{s-1} + g(s),\end{aligned}$$

and we may apply the Tauberian theorem of Appendix II. $\square$

Corollary. (Ideal Theorem) *If $M(x)$ is the number of ideals of R_K with norms bounded by x, then*

$$M(x) = (h\kappa + o(1))x.$$

Proof : Apply the theorem in the case $I = R_K$, and sum the obtained equalities over all classes X of $H^*(K)$. □

This corollary can be also deduced directly from Theorem 7.3 with the use of the tauberian theorem.

In the same manner one can obtain evaluations of the number of prime ideals, or ideals with norms $\leq x$, having certain prescribed properties. Here we prove only one such result:

Proposition 7.19. *Let K be a normal extension of the rationals of degree N, and denote by $F(x)$ the number of integers $n \leq x$ which are norms of ideals of R_K. Then*

$$F(x) = (C + o(1))x(\log x)^{(1-N)/N},$$

where $C = C(K)$ is positive.

Proof : Let $A = N_{K/\mathbb{Q}}(R_K)$, and for $j = 1, 2, \ldots, N$ denote by P_j the set of those rational primes whose jth power is the norm of a prime ideal in R_K. If $m \in A$, then a prime $p \in P_j$ can occur in the factorization of m only with an exponent divisible by j. The normality of $K/\mathbb{Q}$ implies that, conversely, every m satisfying this demand lies in A. This shows that for $\sigma > 1$ we have

$$\sum_{m \in A} \frac{1}{m^s} = \prod_{j=1}^{N} \prod_{p \in P_j} \left(1 + \frac{1}{p^{js}} + \frac{1}{p^{2js}} + \cdots\right) = G(s) \exp\left(\sum_{p \in P_1} \frac{1}{p^s}\right),$$

where

$$G(s) = \exp\left(\sum_{j=2}^{N} \sum_{p \in P_1} \frac{1}{jp^{js}}\right) \prod_{j=2}^{N} \prod_{p \in P_j} \left(1 + \frac{1}{p^{js}} + \frac{1}{p^{2js}} + \cdots\right).$$

Obviously $G(s)$ is regular in $\operatorname{Re} s \geq 1$ and $G(1) \neq 0$. Since P_1 differs only by a finite set of primes from the set of primes splitting in $K/\mathbb{Q}$, Corollary 4 to Proposition 7.16 implies

$$\sum_{p \in P_1} \frac{1}{p^s} = \frac{1}{N} \log \frac{1}{s-1} + g(s),$$

which gives

$$\sum_{m \in A} \frac{1}{m^s} = \frac{g(s)}{(s-1)^{1/N}},$$

with $g(1) \neq 0$. An application of the tauberian theorem leads now to the required result. □

This proposition has an immediate application to the theory of quadratic forms:

Corollary. *Let $K = \mathbb{Q}(\sqrt{D})$ with a square-free D, assume that the class-number $h(K)$ equals 1, and let*

$$F(X,Y) = \begin{cases} X^2 - DY^2 & \text{if } D \equiv 2,3 \pmod 4, \\ X^2 + XY - \frac{D-1}{4}Y^2 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Denote by $f(x)$ the number of natural numbers $n \leq x$ which can be represented in the form $n = \pm F(a,b)$ with rational integral a, b. Then there exists a positive constant $C = C(K)$ such that

$$f(x) = (C + o(1))\frac{x}{\sqrt{\log x}}.$$

Proof : Since $h(K) = 1$, every natural number which is the norm of an ideal of R_K is also the absolute value of the norm of a suitable integer of K. Since the norms of integers are of the form $\pm F(a,b)$ it suffices to apply the proposition. □

3. The results obtained in the preceding subsection do not tell us anything about the size of the remainder terms in asymptotical formulas. Now we shall show that in the case of the Prime Ideal Theorem and its analogue for ideal classes this size is intimately connected with the zero-free region of $\zeta(s,\chi)$. To state this result we shall need the integral logarithm $\operatorname{li} x$ defined by

$$\operatorname{li} x = \int_0^{1-} \frac{dt}{\log t} + \int_{1+}^{x} \frac{dt}{\log t} = \int_2^x \frac{dt}{\log t} - 1.04\ldots .$$

Theorem 7.20. *Let I be a fixed ideal from R_K, X a class of $H_I^*(K)$, and Z_I the set of all function $\zeta(s,\chi)$ associated with characters of $H_I^*(K)$. Moreover, fix $a, b \geq 0$, $A > 0$, $t_0 > e$ and $\epsilon_0 > 0$ and let Ω be the union of the sets*

$$\{s : |t| \geq t_0, \sigma \geq 1 - A(\log|t|)^{-a}(\log\log|t|)^{-b}\}$$

and

$$\{\sigma + it : \ |t| < t_0, \sigma \geq 1 - A(\log|t_0|)^{-a}(\log\log|t_0|)^{-b}, |s-1| \geq \epsilon_0\}.$$

If no function $\zeta(s,\chi) \in Z_I$ vanishes in Ω, and for $s \in \Omega$ one has

$$\frac{\zeta'(s,\chi)}{\zeta(s,\chi)} \ll \log^M(|t|),$$

with a positive M, then

$$\pi_X(x) = \frac{1}{h_I^*(K)} \operatorname{li} x + O(x \exp(-B \log^u x (\log\log x)^v)),$$

where B is a positive constant, $u = 1/(1+a)$ and $v = b/(1+a)$.

Proof : Put

$$S(x) = \sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \le x}} \log N(\mathfrak{p}), \quad T(x) = \sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \le x}} \log N(\mathfrak{p}) \log\left(\frac{x}{N(\mathfrak{p})}\right).$$

We shall reduce our problem to the determination of the behaviour of $T(x)$ as x tends to infinity, and this will be approached by the method of complex integration.

Lemma 7.21. *Assume that for x tending to infinity we have an equality of the form*

$$S(x) = \alpha x + O(R(x)),$$

where $\alpha > 0$, and $R(x)$ is a positive function such that for $x \ge x_0$ the ratio $R(x)/\log^2 x$ is increasing. Then

$$\pi_X(x) = \alpha \operatorname{li} x + O\left(\frac{R(x)}{\log x}\right).$$

Proof : We begin with a modified form of partial summation. Consider the difference $S(x)/\log x - \pi_X(x)$ which also may be written in a slightly artificial form as

$$\begin{aligned} &\frac{S(x)}{\log x} - \sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \le x}} \frac{\log N(\mathfrak{p})}{\log N(\mathfrak{p})} \\ &\quad = \sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \le x}} \log N(\mathfrak{p}) \left(\frac{1}{\log x} - \frac{1}{\log N(\mathfrak{p})}\right) \\ &\quad = \sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \le x}} \int_{N(\mathfrak{p})}^{x} \log N(\mathfrak{p}) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt = \int_2^x S(t) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt. \end{aligned}$$

The validity of the last equality can be verified as follows: order the prime ideals $\mathfrak{p} \in X$ with $N(\mathfrak{p}) \le x$ so that $i \le j$ implies $N(\mathfrak{p}_i) \le N(\mathfrak{p}_j)$, and observe that

$$\sum_{\substack{\mathfrak{p}\in X\\ N(\mathfrak{p})\le x}} \int_{N(\mathfrak{p})}^{x} \log N(\mathfrak{p}) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt$$

$$= \sum_{\substack{j\\ N(\mathfrak{p}_j)\le x}} \log N(\mathfrak{p}_j) \sum_{i>j} \int_{N(\mathfrak{p}_{i-1})}^{N(\mathfrak{p}_i)} \frac{d}{dt}\left(\frac{1}{\log t}\right) dt$$

$$= \sum_{\substack{i\\ N(\mathfrak{p}_i)\le x}} \int_{N(\mathfrak{p}_{i-1})}^{N(\mathfrak{p}_i)} \sum_{j\le i-1} \log N(\mathfrak{p}_j) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt$$

$$= \int_2^x S(t) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt.$$

This shows that

$$\pi_X(x) = \frac{S(x)}{\log x} - \int_2^x S(t) \frac{d}{dt}\left(\frac{1}{\log t}\right) dt,$$

and applying our assumption about $S(x)$ we get

$$\pi_X(x) = \alpha \frac{x}{\log x} + O\left(\frac{R(x)}{\log x}\right) - \int_2^x \alpha t \frac{d}{dt}\left(\frac{1}{\log t}\right) dt + O\left(\int_2^x |R(t)| \left|\frac{d}{dt}\left(\frac{1}{\log t}\right)\right| dt\right).$$

Integrating the integral

$$\int_2^x t \frac{d}{dt}\left(\frac{1}{\log t}\right) dt$$

by parts, and evaluating the last terms by $O(R(x)/\log x) + O(1)$ we obtain the assertion of the lemma. □

Our second step consists in the reduction of the problem of asymptotic behaviour of $S(x)$ to that of $T(x)$:

Lemma 7.22. *If with a certain positive c and non-negative c_1, c_2, satisfying $c_1 + c_2 > 0$ we have*

$$T(x) = \alpha x + O(R_1(x)),$$

where

$$R_1(x) = O(x \exp(-c \log^{c_1} x (\log\log x)^{c_2})),$$

then the same evaluation holds for $S(x)$ as well, perhaps with a smaller value of c.

Proof : Let $\delta = \delta(x) = \exp(-(\log^{c_1/2} x (\log\log x)^{c_2/2}))$, and consider the difference $\Delta(x) = T((1+\delta)x) - T(x)$. It equals

$$S(x)\log(1+\delta)+\sum_{\substack{\mathfrak{p}\in X\\ x<N(\mathfrak{p})\le(1+\delta)x}}\log N(\mathfrak{p})\log\left(\frac{(1+\delta)x}{N(\mathfrak{p})}\right),$$

and since the second summand here is non-negative, we obtain

$$S(x)\le\frac{T((1+\delta)x)-T(x)}{\log(1+\delta)}. \tag{7.21}$$

On the other hand $\Delta(x)$ can be written as

$$\log(1+\delta)S((1+\delta)x)+\sum_{\substack{\mathfrak{p}\in X\\ x<N(\mathfrak{p})\le(1+\delta)x}}\log N(\mathfrak{p})\log\left(\frac{x}{N(\mathfrak{p})}\right),$$

and since the second summand is non-negative, we obtain, replacing x by $x/(1+\delta)$,

$$S(x)\ge\frac{T(x)-T(x(1+\delta))}{\log(1+\delta)}. \tag{7.22}$$

Applying to (7.21) and (7.22) our assumption about $T(x)$ we get

$$\begin{aligned}\frac{\alpha\delta}{(1+\delta)\log(1+\delta)}x+O\left(\frac{R_1(x)}{\log(1+\delta)}\right)&\le S(x)\\ &\le\frac{\alpha\delta}{\log(1+\delta)}x+O\left(\frac{R_1(\delta x)}{\log(1+\delta)}\right).\end{aligned}$$

Since $\lim_{x\to\infty}\delta(x)=0$, we obtain immediately the evaluation

$$S(x)=\alpha x+O(x\delta^2)+O(R_1(x)/\delta)+O(\delta x),$$

and our choice of δ implies that the three remainder terms occurring here are $O(x\exp(-c'\log^{c_1}x(\log\log x)^{c_2}))$ with a suitable constant $c'>0$. □

We are thus left with the task of evaluation $T(x)$ with a good remainder term, and here we shall resort to complex integration. Define a function $K(s)=K_X(s)$ for $\sigma>1$ by putting

$$K(s)=\sum_{\mathfrak{p}\in X}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Its relevance to our problem is explained by the first part of the following lemma:

Lemma 7.23. *(i) If I_2 denotes the vertical line $\sigma=2$, then*

$$T(x)=\frac{1}{2\pi i}\int_{I_2}K(s)\frac{x^s}{s^2}ds.$$

(ii) The function $K(s)$ is regular for $\sigma > 1$, and can be continued analytically to the region Ω, where it is regular except for a simple pole at $s = 1$. Moreover one has

$$K(s) = O(|\log^M(|t|)) \quad \text{for} \quad s \in \Omega, |t| \geq \epsilon_1,$$

where ϵ_1 is an arbitrarily fixed positive number.

Proof : To prove (i) observe first that for positive real ξ we have

$$\int_{I_2} \frac{\xi^s}{s^2} ds = \begin{cases} 2\pi i \log \xi & \text{if } \xi > 1, \\ 0 & \text{if } 0 < \xi \leq 1. \end{cases}$$

Therefore

$$\int_{I_2} K(s) \frac{x^s}{s^2} ds = \sum_{\mathfrak{p} \in X} \log N(\mathfrak{p}) \int_{I_2} \left(\frac{x}{N(\mathfrak{p})} \right)^s \frac{ds}{s^2} = 2\pi i T(x),$$

the interchange of summation and integration being allowed by the uniform convergence of the series

$$\sum_{\mathfrak{p} \in X} \frac{\log N(\mathfrak{p})}{s^2 N(\mathfrak{p})^s}$$

to a function integrable along I_2.

To obtain (ii) write for $\sigma > 1$

$$K(s) = \frac{1}{h_I^*(K)} \sum_{\chi} \overline{\chi}(X) \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p}) \log N(\mathfrak{p})}{N(\mathfrak{p})^s}, \tag{7.23}$$

where χ runs over all characters of $H_I^*(K)$. In the same half-plane we have also for every character χ

$$\zeta(s, \chi) = \exp\left(\sum_{\mathfrak{p}} \frac{\chi(p}{N(\mathfrak{p})^s} + \sum_{p} \sum_{j=2}^{\infty} \frac{\chi^j(\mathfrak{p})}{j N(\mathfrak{p})^{js}} \right),$$

which easily implies the equality

$$\frac{\zeta'(s, \chi)}{\zeta(s, \chi)} = -\sum_{\mathfrak{p}} \sum_{j=2}^{\infty} \frac{\chi^j(\mathfrak{p}) \log N(\mathfrak{p})}{j N(\mathfrak{p})^{js}},$$

where the last term is regular and bounded in Ω. This fact in conjunction with (7.23) leads to the equality

$$K(s) = -\frac{1}{h_I^*(K)} \sum_{\chi} \overline{\chi}(X) \frac{\zeta'(s, \chi)}{\zeta(s, \chi)} + G(s), \tag{7.24}$$

where $G(s)$ is regular and bounded in Ω. This gives the required continuation of $K(s)$ to Ω, and the asserted evaluation is a consequence of the assumptions of Theorem 7.20. □

Now let $T \geq t_0$ be a positive number, whose exact value will be fixed later, put $\phi(t) = A \log^{-1} |t| (\log \log |t|)^{-b}$ and consider the boundary Γ of the set

$$\{s : \ s \in \Omega, \sigma \leq 2, |t| \leq T\},$$

which can be written as $\Gamma = \bigcup_{j=0}^{5} \Gamma_j$, where

$$\begin{aligned}
\Gamma_0 &= \{2 + ti : \ |t| \leq T\}, \\
\Gamma_1 &= \{\sigma + Ti : \ 1 - \phi(T) \leq \sigma \leq 2\}, \\
\Gamma_2 &= \{1 - \phi(t) + ti : \ T \geq |t| \geq t_0\}, \\
\Gamma_3 &= \{1 - \phi(t_0) + it : \ |t| \leq t_0\},
\end{aligned}$$

and Γ_4, Γ_5 are symmetrical images of Γ_2, Γ_1 with respect to the real axis.

We prove now that the integral occurring in Lemma 7.23 (i) is for large T well approximated by the integral of $K(s)x^s/s^2$ over Γ_0, and to deal with that integral we utilize Cauchy's theorem.

Lemma 7.24. *We have*

$$\begin{aligned}
T(x) = \frac{1}{h_I^*(K)} x - \frac{1}{2\pi i} \int_{\Gamma_2 \cup \Gamma_4} \frac{K(s)x^2}{s^2} ds \\
+ O(x^{1-\phi(t_0)}) + O\left(\frac{x^2 \log^M T}{T^2 \log x} \right).
\end{aligned}$$

Proof : First observe that for $s \in I_2$ one has $|K(s)| \leq K(2)$, and thus the preceding lemma implies

$$\begin{aligned}
&|2\pi i T(x) - \int_{\Gamma_0} \frac{K(s)x^s}{s^2} ds| \\
&= O\left(\int_T^\infty \frac{x^2}{4+t^2} dt \right) = O\left(\frac{x^2}{T} \right),
\end{aligned}$$

hence it remains to evaluate the integral over Γ_0.

To do this observe that (7.24) shows that the only singularity of the integrand $K(s)x^s/s^2$ in Ω occurs at $s = 1$, where it has a simple pole with the residue $h_I^*(K)^{-1}$, since the functions $\zeta'(s,\chi)/\zeta(s,\chi)$ are for $\chi \neq \chi_0$ regular in Ω, and for $\chi = \chi_0$ a simple pole occurs at $s = 1$ with residue -1. Cauchy's theorem gives now

$$\frac{1}{2\pi i}\int_{\Gamma_0}\frac{K(s)x^s}{s^2}ds = \frac{1}{2\pi i}\int_{\Gamma}\frac{K(s)x^s}{s^2}ds - \frac{1}{2\pi i}\sum_{j=1}^{5}\int_{\Gamma_j}\frac{K(s)x^s}{s^2}ds$$

$$= \frac{1}{h_I^*(K)}x - \frac{1}{2\pi i}\sum_{j=1}^{5}\int_{\Gamma_j}\frac{K(s)x^s}{s^2}ds.$$

On Γ_1 we have $K(s) = O(\log^M T)$ and $|s|^2 \gg T^2$, thus the integral over Γ_1 is

$$O\left(\frac{\log^M T}{T^2}\int_{1-\phi(T)}^{2} x^u du\right) \ll \left(\frac{x^2\log^M T}{T^2\log x}\right),$$

and the same applies to the integral over Γ_5. Moreover, on Γ_3 we have $|K(s)x^s/s^2| = O(x^{1-\phi(t_0)})$, hence the integral is $O(x^{1-\phi(t_0)})$. □

Finally, we have to evaluate the integrals over Γ_2 and Γ_4. There is nearly no difference between them, and we will consider only the integral over Γ_2 in detail. Obviously we have

$$\int_{\Gamma_2}\frac{K(s)x^s}{s^2}ds \ll \int_{t_0}^{T}\frac{x^{1-\phi(t)}}{t^2}\log^M t\left|\frac{d}{dt}(1-\phi(t)+it)\right|dt,$$

but

$$\frac{d}{dt}(1-\phi(t)+it) \ll \frac{1}{t\log^{a+1}t(\log\log t)^b}$$

and so our integral is

$$\ll x\int_{t_0}^{T}\frac{\exp(-\phi(t)\log x}{t^2}dt.$$

To deal with the last integral we partition the interval $[t_0, T]$ into two subintervals $[t_0, U]$ and $[U, T]$ with

$$U = \exp(A\log^{1/(1+a)}x(\log\log x)^{-b/(1+a)}).$$

Since $\phi(t)$ decreases and is positive, the integral over $[t_0, U]$ is

$$\ll x\exp(-\phi(U)\log x) \ll \exp(-A_1\log^{1/(1+a)}x(\log\log x)^{-b/(1+a)})$$

for a suitable $A_1 > 0$, and the integral over $[U, T]$ is

$$\ll \int_U^{\infty}\frac{dt}{t^2} = \frac{1}{U} \ll \exp(-A_1\log^{1/(1+a)}x(\log\log x)^{-b/(1+a)}).$$

Using Lemma 7.24 we obtain

$$T(x) = \frac{1}{h_I^*(K)}x + O\left(\frac{x^2}{T}\right) + O(x^{1-\phi(t_0)}) + O\left(\frac{x^2 \log^M T}{T^2 \log x}\right)$$
$$+O(x\exp(-A_2 \log^{1/(1+a)} x(\log\log x)^{-b/(1+a)}),$$

and now it is time to choose T. Putting $T = x^2$ one sees that the last remainder term dominates, thus we get

$$T(x) = \frac{1}{h_I^*(K)}x + O(x\exp(-A_2 \log^{1/(1+a)} x(\log\log x)^{-b/(1+a)})),$$

and to conclude the proof one applies the Lemmas 7.21 and 7.22. □

To make the contents of Theorem 7.20 non-void we prove now that its assumption can be satisfied with $a = 1$, $b = 0$, and this will lead to the following result:

Corollary 1. *(i) If X is a class in $H_I^*(K)$, then with a certain constant $B = B(I)$ we have*

$$\pi_X(x) = \frac{\operatorname{li} x}{h_I^*(K)} + O(\exp(-B\sqrt{\log x})).$$

(ii) We have

$$\pi_K(x) = \operatorname{li} x + O(\exp(-B'\sqrt{\log x})),$$

with a constant $B' = B'(K)$.

Proof : We shall verify the assumptions of the theorem for the set Ω with $a = 1$ and $b = 0$, and look first for zeros of $\zeta(s,\chi)$ in Ω. Note that since there are only finitely many characters χ involved, it suffices to do this for each particular χ. Since $\zeta(\overline{s},\overline{\chi}) = \overline{\zeta(s,\chi)}$ (which is obvious for $\sigma > 1$ and for other s follows by analytic continuation), we may restrict our attention to zeros in the upper half-plane. Moreover, we will not bother about zeros with small imaginary parts, since by a change of the constant A in the definition of Ω we can keep them outside that region. Thus let $z_0 = \xi + i\eta$ be a root of $\zeta(s,\chi)$, with $\xi \geq 7/8$, $\eta \geq 3$, and write $\xi = 1 - c/\log\eta$. We have to show that c exceeds a positive constant, independent of the chosen zero z_0, but which may depend on χ, since we are not interested in a uniform result. We apply Theorem III of Appendix II, taking $f(s) = \zeta(s,\chi)$, $s_0 = \tau + i\eta$ with $\tau = 1 + \alpha/\log\eta$, where $0 < \alpha < 1/2$ (the precise value of α will be fixed later) and $r = 1/2$. Since $\eta \geq 3$, the only possible singular point of $\zeta(s,\chi)$, viz. $s = 1$, lies outside the disc $D = \{s : |s - s_0| \leq 1/2\}$, and, moreover, $\zeta(s,\chi)$ does not vanish in the half-plane $\sigma \geq \tau > 1$. So we need only a bound for $|\zeta(s,\chi)/\zeta(s,\chi_0)|$ in D. This is provided by the following argument:

Theorem 7.13 gives for every $\epsilon > 0$ the evaluation

$$|\zeta(s,\chi)| \ll |t|^{N/2+\epsilon}$$

with $N = [K : \mathbb{Q}]$, and since for $\sigma > 1$ we have the identity

$$\frac{1}{\zeta(s,\chi)} = \sum_I \frac{\chi(I)\mu_K(I)}{N(I)^s},$$

which is easily proved by multiplying the series occurring in it, we get

$$\left|\frac{1}{\zeta(s_0,\chi)}\right| \ll \zeta_K(s_0) \ll \frac{\log\eta}{\alpha}.$$

This yields

$$\left|\frac{\zeta(s,\chi)}{\zeta(s_0,\chi)}\right| \ll \eta^{N/2+\epsilon}\frac{\log\eta}{\alpha},$$

and applying Theorem III of Appendix II, we obtain with certain positive B and B_1

$$\begin{aligned}&\text{Re } (\zeta'(s_0,\chi)/\zeta(s,\chi))\\ &\geq -8(\log B - \log a + (N/2+\epsilon)\log\eta + \log\log\eta) + (\tau-\xi)^{-1}\\ &\geq B_1(\log a + \log\eta) + (\tau-\xi)^{-1}.\end{aligned}$$

We apply the same procedure to the point $\tau + 2i\eta$, again with $r = 1/2$, but this time with the function $f(s) = \zeta(s,\chi^2)$, and similarly we obtain the evaluation

$$\text{Re}\left(\frac{\zeta'(\tau+2i\eta,\chi^2)}{\zeta(\tau+2i\eta,\chi^2)}\right) \geq -B_2(\log\eta - \log\alpha),$$

for a suitable $B_2 > 0$.

Now observe that

$$\text{Re}\left(3\frac{\zeta'(\tau,\chi_0)}{\zeta(\tau,\chi_0)} + 4\frac{\zeta'(\tau+i\eta,\chi)}{\zeta(\tau+i\eta,\chi)} + \frac{\zeta'(\tau+2i\eta,\chi^2)}{\zeta(\tau+2i\eta,\chi^2)}\right) \leq 0. \tag{7.25}$$

In fact, taking the logarithmic derivative of the Euler product of our zeta-function we see that for $\sigma > 1$ one has

$$\zeta'(s,\chi)/\zeta(\sigma,\chi) = -\sum_I \frac{\chi(I)a(I)}{N(I)^s},$$

where

$$a(I) = \begin{cases}\log N(\mathfrak{p}) & \text{if } I \text{ is a power of } \mathfrak{p},\\ 0 & \text{otherwise.}\end{cases}$$

Substituting this series into the left-hand side of (7.25) we obtain

$$-\sum_I \frac{a(I)}{N(I)^\tau}\text{Re}\left(3\chi_0(I) + \frac{4\chi(I)}{N(I)^{i\eta}} + \frac{\chi^2(I)}{N(I)^{2i\eta}}\right)$$

$$= -\sum_I \frac{a(I)}{N(I)^\tau}\text{Re}\,(3+4\cos\lambda_I+\cos(2\lambda_I)) = -2-2\sum_I \frac{a(I)(1+\cos\lambda_I)^2}{N(I)^\tau} \leq 0,$$

where α_I denotes the argument of $\chi(I)N(I)^{-i\eta}$. The resulting inequality implies

$$-3\mathrm{Re}\,(\zeta'(\tau,\chi_0)/\zeta(\tau,\chi_0)) \geq \frac{4}{\tau-\xi} - B_3(\log\eta - \log\alpha).$$

On the other hand, expanding $\zeta'(s,\chi_0)/\zeta(s,\chi_0)$ at $s=1$ we obtain

$$3\mathrm{Re}\,(\zeta'(s,\chi_0)/\zeta(s,\chi_0)) = \frac{-3}{s-1} + c_0 + c_1(s-1) + \cdots,$$

and this shows that for every $\epsilon > 0$ we have

$$3\mathrm{Re}\,(\zeta'(\tau,\chi_0)/\zeta(\tau,\chi_0)) \geq -\frac{3+\epsilon}{\tau-1},$$

provided $\tau - 1$ is sufficiently small. Now we have two inequalities for the same expression, and we shall prove their inconsistency for sufficiently small c and suitably chosen α. The comparison of these inequalities yields

$$\frac{3+\epsilon}{\tau-1} \geq \frac{4}{\tau-\xi} - B_3(\log\eta - \log a),$$

but $\tau - \xi = (\alpha + c)\log\eta$, and $\tau - 1 = \alpha/\log\eta$, thus

$$(3+\epsilon)\log\eta/\alpha + B_3(\log\eta - \log\alpha) \geq 4\frac{\log\eta}{a+c},$$

and we arrive finally at

$$\begin{aligned} -B_3\log\alpha &> \left(\frac{4}{a+c} + \frac{3+\epsilon}{\alpha} + B_3\right)\log\eta \\ &\geq \left(\frac{4}{a+c} + \frac{3+\epsilon}{\alpha} + B_3\right)\log 3. \end{aligned} \tag{7.26}$$

If now a sufficiently small α is fixed, then $B_3\log(1/\alpha) \leq 1/\alpha$, but if we let in (7.26) the number c tend to zero, then we get

$$\frac{1}{\alpha} > \frac{4\log 3 + (3+\epsilon)\log 3}{\alpha} + B_3\log 3,$$

which is not possible for sufficiently small α.

We have thus obtained a zero-free region Ω with $a = 1$, $b = 0$ and certain $A > 0$. Now let Ω' be the region defined similar to Ω, but with A replaced by $4A$. Since Ω' is contained in Ω, it is a zero-free region for $\zeta(s,\chi)$, hence $f(s) = \log\zeta(s,\chi)$ is regular there, and we shall show that for $s \in \Omega'$ one has the bound $O(\log^M|t|)$ for the logarithmic derivative of $\zeta(s,\chi)$. Clearly it suffices to do so in the case $t > 0$.

Let C be a large positive number, and consider a point $a = \alpha + \beta i \in \Omega'$ with $\beta \geq C$ and $\alpha \leq 1$. Put $s_0 = 2 + i\beta$, and consider the disc $D = \{s : |s - s_0| \leq 1 + 1/(2A\log\beta)\}$. Since $D \subset \Omega'$, we may apply Theorem IV of

Appendix II to our function $f(s)$ and s_0, with $R = 1 + 1/(2A\log\beta)$ and $r = 1 + 1/(3A\log\beta)$. Since $R \le 2$, $|f(s_0)| = O(1)$ and, by Theorem 7.13,

$$\max_{|s-s_0|\le R} \operatorname{Re} f(s)$$
$$\le \log \max\{|\zeta(s,\chi)| : \ 0 \le \tau \le 4, t-2 \le \operatorname{Im} s \le t+2\} \ll \log t,$$

the said theorem of the appendix implies $|f(s)| \ll \log^2 t$ for all s with $|s-s_0| < 1_1/(3A\log t)$. Finally, note that if $|s-s_0| = R$ then $|z-s| \ge 1/(12A\log t)$, hence

$$|f'(z)| = \frac{1}{2\pi}\left|\int_{|s-s_0|=R} \frac{f(s)}{(z-s)^2} ds\right| \le R\log^2 t \cdot 144A^2\log^2 t = O(\log^4 t),$$

and this is all we need for the proof of (i). The assertion (ii) is an immediate consequence. □

Corollary 2. *One has*

$$\pi_K(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$$

and

$$\pi_K(x) = \operatorname{li} x + O\left(\frac{x}{\log^N x}\right)$$

for every N. □

4. Now we shall use Corollary 7 to Proposition 7.16 to prove a result of N.Moser [83], concerning Minkowski units. Let us recall that if the extension $K/\mathbb{Q}$ is normal with Galois group G, then a unit of K is called a *Minkowski unit*, if its image in the group $U(K)/E(K)$ generates this group as a $\mathbb{Z}[G]$-module. In Theorem 3.28 we considered the case when G was cyclic of prime order $p \le 19$, and now we turn to dihedral group D_n of order $2n$, which can be defined as the group of motions of the regular n-gon, or, equivalently, as the group generated by two elements S, T with relations

$$S^n = T^2 = 1, \quad TS = S^{-1}T.$$

Note that for T one can choose any element of order 2 in D_n.

Theorem 7.25. *Every complex normal extension $K/\mathbb{Q}$ whose Galois group G is isomorphic to D_p (with p being an odd prime) has a Minkowski unit.*

Proof : Denote by R the ring of integers of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, and let A be the R-module consisting of all linear polynomials in one variable with coefficients in R. Defining a multiplication in A by

$$(a+bX)(c+dX) = (ac+b\overline{d}) + (ad+b\overline{c})X$$

(with $\overline{z}$ being the complex conjugate of z) we make A into a ring, clearly non-commutative. The following lemma shows that A is an epimorphic image of $\mathbb{Z}[G]$, hence can be regarded as a $\mathbb{Z}[G]$-module:

Lemma 7.26. *The map $S \mapsto \zeta_p$, $T \mapsto X$ can be extended to a surjective ring homomorphism $\varphi : \mathbb{Z}[G] \longrightarrow A$, whose kernel equals $N_H\mathbb{Z}[G]$, where H is the subgroup of G generated by S, and*

$$N_H = \sum_{h \in H} h = 1 + S + S^2 + \cdots + S^{p-1}.$$

Proof : Every element of D_p can be uniquely written in the form S^k, or S^kT with $0 \leq k \leq p-1$, hence the formula

$$\varphi\left(\sum_{j=0}^{p-1}(a_jS^j + b_jS^jT)\right) = \sum_{j=0}^{p-1}\zeta_p^j(a_j + b_jX), \quad (a_j, b_j \in \mathbb{Z})$$

defines a linear map of $\mathbb{Z}[G]$ onto A. One checks easily that it is a ring homomorphism.

If $u = \sum_{j=0}^{p-1}(a_jS + b_jS^jT)$ lies in the kernel of φ, then

$$\sum_{j=0}^{p-1} a_j\zeta_p^j = \sum_{j=0}^{p-1} b_j\zeta_p^j = 0,$$

hence

$$\sum_{j=0}^{p-2}(a_j - a_{p-1})\zeta_p^j = 0.$$

But $1, \zeta_p, \ldots, \zeta_p^{p-2}$ is an integral basis of R, thus all a_i's must be equal, and the same applies to the b_i's. This shows that $u = (a_0 + b_0T)N_H \in \mathbb{Z}[G]N_H = N_H\mathbb{Z}[G]$, because N_H lies in the center of $\mathbb{Z}[G]$. In fact, it suffices to check that N_H commutes with every $g \in G$, and this follows from the observation that H is of index 2 in G, and thus is a normal subgroup.

This shows that the kernel of φ lies in $N_H\mathbb{Z}[G]$, and the converse results from $\varphi(N_H) = 0$. □

Before proceeding further observe that we can assume that T acts on K as complex conjugation. We shall use this in the proof of the next lemma, which will allow us to induce the structure of an A-module on $U(K)/E(K)$.

Lemma 7.27. *If $k \subset K$ corresponds to H by Galois theory, then k is imaginary quadratic, thus the group $U(k)/E(k)$ is trivial.*

Proof : Since H is of index 2, k is a quadratic extension of $\mathbb{Q}$. The field k_0, corresponding to the subgroup H_0 generated by T is the maximal real subfield of K, Because of $H \cap H_0 = 1$, we have $K = kk_0$, and if k were real, K would be real as well, contrary to our assumption. Hence k is imaginary quadratic, and the last assertion follows immediately. □

Corollary 1. *The ideal $N_H\mathbb{Z}[G]$ of $\mathbb{Z}[G]$ annihilates $U(K)/E(K)$, i.e., for every $a \in N_H\mathbb{Z}[G]$ and $u \in U(K)/E(K)$ we have $au = 1$.*

Proof : It suffices to observe that for a unit u of K we have

$$N_H \cdot u = \prod_{j=0}^{p-1} S^j(u) = N_{K/k}(u) \in U(k) = E(k) \subset E(K). \qquad \square$$

Corollary 2. *The action of $\mathbb{Z}[G]$ induces on $U(K)/E(K)$ the structure of an A-module.*

Proof : This follows from Corollary 1 and Lemma 7.26. □

Since R is a subring of A, the last corollary shows that $U(K)/E(K)$ is a torsion-free and finitely generated R-module. We may thus invoke Theorem 1.32 to obtain the existence of an ideal J of R such that $U(K)/E(K)$ is isomorphic as an R-module to $R^m \oplus J$ with a suitable $m \geq 0$. Comparing the $\mathbb{Z}$-ranks we get $p - 1 = (m + 1)(p - 1)$, hence $m = 0$ and $U(K)/E(K) \sim J$. This isomorphism induces on J an A-module structure, and so we may regard J as a $\mathbb{Z}[G]$-module by Lemma 7.26. To prove the theorem it suffices now to show that J is a cyclic module, i.e., is generated by one element.

The action of A on J is determined by the action of X, since the elements of R act on J by multiplication. We show now that there is an element $c \in \mathbb{Q}(\zeta_p)$ of absolute value 1 such that the element X acts on $z \in J$ by $X(z) = c\overline{z}$. If $r \in R$, $r \neq 0$ and $z \in J$, $z \neq 0$, then

$$X(rz) = (Xr)z = (\overline{r}X)z = \overline{r}X(z),$$

hence if $r, z \in J$ $rz \neq 0$, then

$$\overline{r}X(z) = X(rz) = X(zr) = \overline{z}X(r),$$

implying $X(r)/\overline{r} = X(z)/\overline{z} = c$, with a certain c, independent of r and z. This leads to $X(z) = c\overline{z}$ for all $z \in J$, since for $z = 0$ this equality is evident. If now z_0 is the image of a real unit in J, then $X(z_0) = z_0$, because on $U(K)/E(K)$ the element X acts as complex conjugation. Hence $c\overline{z}_0 = z_0$ and we get $|c| = 1$.

Since $c\overline{J} = X(J) \subset J$, we obtain

$$\overline{J} = c\overline{c}\overline{J} \subset \overline{c}J \subset \overline{J},$$

i.e., $\overline{c}J = \overline{J}$, thus $X(J) = J = c\overline{J}$. We will use this to show that in the class of J there is an ideal I satisfying $\overline{I} = I$. The function $x + \overline{cx}$ obviously cannot vanish identically on R, thus there exists $x_0 \in R$ such that $a = x_0 + \overline{cx}_0 \neq 0$. Since $\overline{a} = \overline{x}_0 + cx_0$, we obtain $\overline{ca} = a$, thus $\overline{c} = a/\overline{a}$. Consider the ideal $I = qaJ$, where q is a positive rational integer such that $qa \in R$. Then I and J lie in the same class, and, moreover, $\overline{I} = q\overline{a}J = I$, as needed. Since Theorem 1.39 implies $I \sim J$, we see that $U(K)/E(K)$ and I are isomorphic R-modules. We may thus replace J by I, or, which is simpler, assume that $\overline{J} = J$. This gives $cJ = J$, and consequently c is a unit of R. Now choose an unramified prime ideal $\mathfrak{p} \subset R$ of first degree in such a way that the ideal $\mathfrak{p}J = xR$ is principal, Such a choice is possible by Corollary 7 to Proposition 7.16. Note that, in particular, we have $\overline{\mathfrak{p}} \neq \mathfrak{p}$, hence $(\mathfrak{p}, \overline{\mathfrak{p}}) = 1$.

If now

$$u = \sum_{j=0}^{p-1} (a_j S^j + b_j S^j T) \quad (a_i, b_i \in \mathbb{Z})$$

is an arbitrary element of $\mathbb{Z}[G]$ then

$$ux = \sum_{i=0}^{p-1} a_i \zeta_p^i x + \sum_{i=0}^{p-1} b_i \zeta_p^i \overline{x},$$

hence

$$\mathbb{Z}[G]x = Rx + R\overline{x} = \mathfrak{p}J + \overline{\mathfrak{p}}\overline{J} = J(\mathfrak{p} + \overline{\mathfrak{p}}) = JR = J,$$

showing that J is generated by x as a $\mathbb{Z}[G]$-module. □

7.3. Chebotarev's Theorem

1. In Chap. 6 we have seen that to every prime ideal $\mathfrak{P}$ in a normal extension L/K of an algebraic number field there corresponds a canonically determined subgroup of the Galois group G, namely the decomposition group $G_{-1}(\mathfrak{P})$, which is isomorphic in a natural way to the Galois group of the corresponding local extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. In the case of unramified $\mathfrak{P}$ Theorem 5.25 shows that this group is isomorphic to the Galois group of the corresponding extension of the finite field $R_K/\mathfrak{p}$, which is necessarily cyclic. It follows from the theory of finite fields that this group has a distinctive generator s acting by $s(a) = a^{p^F}$, where $F = f(K_{\mathfrak{p}}/\mathbb{Q}_p)$. We can trace down this generator to $G_{-1}(\mathfrak{P})$ through our isomorphisms, and so we obtain an automorphism $s_{\mathfrak{P}}$ of L/K, satisfying

$$s_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for all $x \in R_L$. Note that this property determines $s_{\mathfrak{P}}$ uniquely. Traditionally $s_{\mathfrak{P}}$ is denoted by

$$\left[\frac{L/K}{\mathfrak{P}}\right],$$

and called the *Frobenius automorphism* associated with $\mathfrak{P}$, or the *Frobenius symbol*.

If we take another prime ideal lying over the same prime ideal $\mathfrak{p}$, then the corresponding Frobenius automorphisms may differ, but are still related.

Proposition 7.28. *If t is an element of the Galois group $Gal(L/K)$, then*

$$\left[\frac{L/K}{t(\mathfrak{P})}\right] = t \circ \left[\frac{L/K}{\mathfrak{P}}\right] \circ t^{-1}.$$

Proof : If $x \in R_L$, then $s_{\mathfrak{P}}(x) - x^{N(\mathfrak{p})}$ lies in $\mathfrak{P}$, hence

$$t \circ s_{\mathfrak{P}} \circ t^{-1}(x) - t \circ t^{-1}(x^{N(\mathfrak{p})}) \in t(\mathfrak{P}),$$

i.e.,

$$t \circ s_{\mathfrak{P}} \circ t^{-1}(x) - x^{N(\mathfrak{p})} \in t(\mathfrak{P}),$$

proving the proposition. □

Corollary. *If L/K is Abelian, then the Frobenius automorphism of $\mathfrak{P}$ depends only on the prime ideal $\mathfrak{p}$ of R_K lying below $\mathfrak{P}$.* □

If L/K is normal, and for any $g \in Gal(L/K)$ we denote by $Cl(g)$ the conjugacy class of g, i.e., the set of all elements conjugated with g, then one defines a map $F_{L/K}$ of the set of all prime ideals of R_K, unramified in L/K, into the set of all conjugacy classes in $Gal(L/K)$ by putting

$$F_{L/K} : \mathfrak{p} \mapsto Cl(s_{\mathfrak{P}}),$$

where $\mathfrak{P}$ is an arbitrary prime ideal of R_L lying above $\mathfrak{p}$. The following theorem gives the main properties of this map:

Theorem 7.29. *(i) If L/K is normal of degree n, the prime ideal $\mathfrak{p}$ of R_K is unramified in L/K, and f is the order of any element of $F_{L/K}(\mathfrak{p})$, then*

$$\mathfrak{p}R_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \quad f_{L/K}(\mathfrak{P}) = f,$$

where $g = n/f$.

(ii) If $K \subset L \subset M$, M/K and L/K are normal, $\mathfrak{p}$ is a prime ideal of R_K unramified in M/K and $R = R_{M/L} : Gal(M/K) \longrightarrow Gal(L/K)$ is the restriction map, then $R(F_{M/K}(\mathfrak{p})) = F_{L/K}(\mathfrak{p})$.

(iii) If L/K and M/K are normal, and $\mathfrak{p}$ is a prime ideal of R_K unramified in LM/K, then the inclusion

$$F_{LM/K}(\mathfrak{p}) \subset F_{L/K}(\mathfrak{p})F_{M/K}(\mathfrak{p})$$

holds, provided we identify the group $Gal(LM/K)$ *with its image under the map* $s \mapsto [s_{|L}, s_{|M}]$ *in the product* $Gal(L/K) \times Gal(M/K)$.

(iv) If L/K *is normal,* M/K *is finite,* $\mathfrak{p}$ *is a prime ideal of* R_K *unramified in* L/K, *and* $\mathfrak{q}$ *is a prime ideal of* R_M, *lying above* $\mathfrak{p}$, *then* $\mathfrak{q}$ *is unramified in* LM/M, *and we have*

$$F_{LM/M} \subset F_{L/K}(\mathfrak{p})^f,$$

where $f = f_{M/K}(\mathfrak{q})$.

(v) Let L/K *be finite, and let* M/K *be the minimal normal extension of* K *containing* L. *Let* $\mathfrak{p}$ *be a prime ideal of* R_K *unramified in* L/K, $\mathfrak{P}$ *a prime ideal of* R_M *lying above* $\mathfrak{p}$, *and* $\mathfrak{Q}$ *the prime ideal of* R_L *lying below* $\mathfrak{P}$. *Put also* $s = \left[\frac{M/K}{\mathfrak{P}}\right]$, *and let* H *be the subgroup of* $Gal(M/K)$ *generated by* s. *Then*

$$f_{L/K}(\mathfrak{Q}) = \frac{\#H}{\#(H \cap U)},$$

where U *is the subgroup of* $Gal(M/K)$ *corresponding to* L *according to Galois theory. Moreover, the set of prime ideals of* R_M *lying over* $\mathfrak{Q}$ *coincides with the set* $\{us^k(\mathfrak{P}) : \ u \in U, k \geq 0\}$

Proof: (i) Since $e_{L/K}(\mathfrak{P}) = 1$, and $\left[\frac{L/K}{\mathfrak{P}}\right]$ generates the decomposition group of $\mathfrak{P}$, the assertion follows from the Corollary 1 to Proposition 6.8.

(ii) If $s \in F_{M/K}(\mathfrak{p})$, $s_1 = R(s)$, and $\mathfrak{P}$ lies over $\mathfrak{p}$ in R_M, then for $x \in R_L$ we have $s_1(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$. This implies $s_1(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}_1}$ for $x \in R_L$, where $\mathfrak{P}_1$ lies below $\mathfrak{P}$ in R_L, and therefore $s_1 \in F_{L/K}(\mathfrak{p})$. We see that R maps $F_{M/K}(\mathfrak{p})$ into $F_{L/K}(\mathfrak{p})$, and since it is surjective and preserves conjugacy classes, we get $R(F_{M/K}(\mathfrak{p})) = F_{L/K}(\mathfrak{p})$.

(iii) Observe that the map $Gal(LM/K) \longrightarrow Gal(L/K) \times Gal(M/K)$ given by $g \mapsto [g_{|L}, g_{|M}]$ is injective, and the composition of it with the projection onto $Gal(L/K)$, resp. $Gal(M/K)$, coincides with $R_{LM/L}$ and $R_{LM/M}$, respectively. Applying this to $g \in F_{LM/K}(\mathfrak{p})$, we get

$$g = [g_{|L}, g_{|M}] = [R_{LM/L}(g), R_{LM/M}(g)] \subset F_{L/K}(\mathfrak{p})F_{M/K}(\mathfrak{p})$$

by (ii).

(iv) If g is an element of $Gal(LM/M)$, then $g_{|L}$ lies in $Gal(L/L \cap M)$, and the map $g \mapsto g_{|L}$ is an isomorphism. We can thus identify $Gal(LM/M)$ and $Gal(L/L \cap M)$. Applying Corollary 1 to Lemma 5.24 to the corresponding $\mathfrak{p}$-adic extension, and using Theorem 5.11 (iv), we see that $\mathfrak{q}$ is unramified in LM/M, proving the first part of our assertion. To prove the second take $g \in F_{LM/M}(\mathfrak{q})$, and let $\mathfrak{P}_1$ be that prime ideal in R_{LM} which lies over $\mathfrak{q}$, and satisfies

$$\left[\frac{LM/M}{\mathfrak{P}_1}\right] = g.$$

If $\mathfrak{P}$ is the prime ideal of R_L lying below $\mathfrak{P}_1$, then for $x \in R_L$ we have

$$x^{N(\mathfrak{q})} \equiv g(x) \pmod{\mathfrak{P}_1},$$

and the same congruence holds also mod $\mathfrak{P}$. If we choose $g_1 \in F_{L/K}(\mathfrak{p})$ so that the congruence

$$x^{N(\mathfrak{p})} \equiv g_1(x) \pmod{\mathfrak{P}}$$

holds, then in view of $N(\mathfrak{q}) = N(\mathfrak{p})^f$ we get

$$x^{N(\mathfrak{q})} \equiv g_1^f(x) \pmod{\mathfrak{P}},$$

and this leads to

$$g(x) \equiv g_1(x) \pmod{\mathfrak{P}},$$

which can hold for all $x \in R_L$ only if g and g_1^f coincide. But this shows that $F_{LM/M}(\mathfrak{q}) \subset F_{L/K}(\mathfrak{p})^f$, as required.

(v) Observe first that by Corollary 2 to Proposition 4.25 the prime ideal $\mathfrak{P}$ is unramified in M/K. The elements s^k $(k = 0, 1, \ldots)$ belong to the decomposition group of $\mathfrak{P}$ over K, thus $s^k(\mathfrak{P}) = \mathfrak{P}$, and if $u \in U$ and $\mathfrak{P}_1 = u(\mathfrak{P})$, then from $\mathfrak{Q}R_M \subset \mathfrak{P}$ we get $u(\mathfrak{Q}R_M) \subset \mathfrak{P}_1$, which in view of $u(\mathfrak{Q}) = \mathfrak{Q}$ gives $\mathfrak{Q}R_M \subset \mathfrak{P}_1$. Hence $\mathfrak{P}_1$ lies over $\mathfrak{Q}$. This shows that all ideals $(us^k)(\mathfrak{P})$ lie over $\mathfrak{Q}$. To show that no other prime ideal can lie over $\mathfrak{Q}$ observe that if $\mathfrak{P}'$ has this property, then with a suitable $u \in Gal(M/L) = U$ we have $\mathfrak{P}' = u(\mathfrak{P})$.

Finally, Lemma 6.7 shows that the decomposition group of $\mathfrak{P}$ over K equals $H \cap U$, and so we obtain

$$f_{K/\mathbb{Q}}(\mathfrak{Q}) = f_{M/K}(\mathfrak{P})/f_{M/L}(\mathfrak{P}) = \frac{\#H}{\#(H \cap U)}. \qquad \square$$

Corollary 1. *A prime ideal $\mathfrak{p} \subset R_K$ splits in a normal extension L/K if and only if $F_{L/K}(\mathfrak{p}) = 1$.*

Proof : Immediate from (i). $\square$

The next corollary explains the example presented after the Corollary 5 to Proposition 7.16.

Corollary 2. *If L/K is normal, then a prime ideal $\mathfrak{p}$ of R_K remains a prime ideal in R_L if and only if the Galois group of L/K is cyclic and generated by $F_{L/K}(\mathfrak{p})$.*

Proof : A prime ideal $\mathfrak{p}$ of R_K remains prime in R_L if and only if it is unramified, and for every prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ in R_L we have $f_{L/K}(\mathfrak{P}) = [L : K]$. In view of (i) this implies our assertion. $\square$

Corollary 3. *If L/K is finite, and M/K is the minimal normal extension of K containing L, then the type of factorization (i.e., the number and degrees of the factors) of a prime ideal of R_K, unramified in L/K, depends solely on the subgroup of $Gal(M/K)$, corresponding to L, and $F_{M/K}(\mathfrak{p})$.*

Proof : Apply (i) and (v). □

2. The principal result concerning the Frobenius automorphism is the *density theorem of Chebotarev*, which we first present in its weaker form:

Theorem 7.30. *If L/K is normal of degree n, and A is a conjugacy class in the Galois group $Gal(L/K)$, then the set*

$$P_A = \{\mathfrak{p} : \ F_{L/K}(\mathfrak{p}) = A\}$$

is infinite, and has Dirichlet density $\#A/n$.

The stronger form requires for its proof Artin's reciprocity law, which lies outside the scope of this book. Chebotarev's theorem in its stronger form reads as follows:

Theorem 7.30*. *If L/K is normal of degree n, and A is a conjugacy class in the Galois group $Gal(L/K)$, then the set*

$$P_A = \{\mathfrak{p} : \ F_{L/K}(\mathfrak{p}) = A\}$$

is regular, and has Dirichlet density $\#A/n$. If $N_A(x)$ is the number of prime ideals $\mathfrak{p} \in P_A$ with $N(\mathfrak{p}) \leq x$, then

$$N_A(x) = \left(\frac{\#A}{n} + o(1)\right) \frac{x}{\log x}.$$

In the case when $K = \mathbb{Q}$, and $L/\mathbb{Q}$ is Abelian, or more generally, when L is contained in a cyclotomic extension of K, one can give an elementary proof of Theorem 7.30*, and this will be the first step towards the proof of Theorem 7.30. In the next step we shall reduce the problem to the case of cyclic extensions, and finally, for a given cyclic extension we shall combine various cyclic extensions contained in cyclotomic extensions to obtain the assertion. In the last step we shall approximate the sum

$$\sum_{\mathfrak{p} \in P_A} N(\mathfrak{p})^{-s},$$

and our approach will not be strong enough to yield the regularity of P_A.

Proof of Theorem 7.30: First we establish Theorem 7.30* for cyclotomic extensions:

Lemma 7.31. *If $L = K(\zeta_m)$, then Theorem 7.30* holds for the extension L/K.*

Proof : Put $K_m = \mathbb{Q}(\zeta_m)$, and apply Theorem 7.29 (iv) to the normal extension $K_m/\mathbb{Q}$ and $K/\mathbb{Q}$. Let $\mathfrak{q}$ be a prime ideal of K lying over $\mathfrak{p} = p\mathbb{Z}$, and assume that $\mathfrak{p}$ does not ramify in $K_m/\mathbb{Q}$, and $f_{K/\mathbb{Q}}(\mathfrak{q}) = 1$. Since both extensions $K_m/\mathbb{Q}$ and L/K are Abelian, the theorem quoted implies $F_{L/K}(\mathfrak{q}) = F_{K_m/\mathbb{Q}}(\mathfrak{p})$, if we consider the Galois group $Gal(L/K)$ as a subgroup of $Gal(K_m/K)$. Now note that every automorphism of K_m is determined by its action on ζ_m, and denote by g_r the automorphism satisfying $g_r(\zeta_m) = \zeta_m^r$ $(1 \le r \le m,\ (r,m) = 1)$. The definition of the Frobenius automorphism implies that $F_{K_m/\mathbb{Q}}(\mathfrak{p}) = g_r$ holds if and only if $p \equiv r \pmod m$. This shows that

$$\begin{aligned} P_r &= \{\mathfrak{q} :\ f_{K/\mathbb{Q}}(\mathfrak{q}) = 1, F_{L/K}(\mathfrak{q}) = g_r\} \\ &= \{\mathfrak{q} :\ f_{K/\mathbb{Q}}(\mathfrak{q}) = 1, N(\mathfrak{q}) \equiv r \pmod m\}, \end{aligned}$$

and thus

$$\sum_{\substack{\mathfrak{q} \\ F_{L/K}(\mathfrak{q}) = g_r}} \frac{1}{N(\mathfrak{q})^s} = \sum_{\mathfrak{q} \in P_r} \frac{1}{N(\mathfrak{q})^s} + g(s) = \sum_{\substack{\mathfrak{q} \\ N(\mathfrak{q}) \equiv r \pmod m}} \frac{1}{N(\mathfrak{q})^s} + g(s),$$

since prime ideals $\mathfrak{q}$ with $f_{L/K}(\mathfrak{q}) \neq 1$ contribute only to $g(s)$ in the equalities above.

Now observe that if a is a totally positive integer of K congruent to unity mod m, then $N_{K/\mathbb{Q}}(a) \equiv 1 \pmod m$. Since a is totally positive we get $N(aR_K) = N_{K/\mathbb{Q}}(a)$, and this implies that the set $\{I :\ N(I) \equiv 1 \pmod m\}$ is a sum of, say, k classes from $H^*_{\mathfrak{m}}(K)$, where $\mathfrak{m} = mR_K$. Therefore the set $\{I :\ N(I) \equiv r \pmod m\}$ is either void, or contains k classes of $H^*_{\mathfrak{m}}(K)$. Corollary 6 to Proposition 7.16 gives now

$$\sum_{\substack{\mathfrak{q} \\ N(\mathfrak{q}) \equiv r \pmod m}} \frac{1}{N(\mathfrak{q})^s} = \frac{\epsilon_r k}{h^*_{\mathfrak{m}}(K)} \log \frac{1}{s-1} + g(s), \tag{7.26}$$

where ϵ_r equals 0 or 1. If we put $l = \epsilon_1 + \cdots + \epsilon_{m-1}$, then the last equality implies $kl = h^*_{\mathfrak{m}}(K)$, but l cannot exceed the order of $Gal(L/K)$, thus

$$nk \ge h^*_{\mathfrak{m}}(K) \tag{7.27}$$

must hold. On the other hand, every prime ideal $\mathfrak{q} \in R_K$ of the first degree with $N(\mathfrak{q}) \equiv 1 \pmod m$ splits in L/K. In fact, in this case we have $F_{K_m/\mathbb{Q}}(\mathfrak{p}) = 1$. Now (7.26) shows that the density of the set of prime ideals splitting in L/K equals at least $kh^*_{\mathfrak{m}}(K)^{-1}$, and by Corollary 3 to Proposition 7.17 it equals $1/n$. Thus

$$nk \le h^*_{\mathfrak{m}}(K),$$

and (7.27) implies that we have equality here. So (7.26) becomes

$$\sum_{\substack{\mathfrak{q} \\ N(\mathfrak{q}) \equiv r \pmod{m}}} \frac{1}{N(\mathfrak{q})^s} = \frac{\epsilon_r}{n} \log \frac{1}{s-1} + g(s),$$

and we see that exactly n of the sets P_r are non-empty. But this proves that every element of $Gal(L/K)$ is the Frobenius automorphism for prime ideals forming a regular set of density $1/n$. □

Using this lemma we obtain now the Theorem 30* for subextensions of cyclotomic extensions:

Lemma 7.32. *If $L = K(\zeta_m)$ and $K \subset M \subset L$, then Theorem 7.30* is true for the extension M/K.*

Proof : Denote by φ the restriction map of $Gal(L/K)$ onto $Gal(M/K)$, and let $\mathfrak{p}$ be a prime ideal of K, unramified in L/K. By Theorem 7.29 (i) we have $F_{M/K}(\mathfrak{p}) = \varphi(F_{L/K}(\mathfrak{p}))$, and so for $g \in Gal(M/K)$ we obtain

$$\sum_{\substack{\mathfrak{p} \\ F_{M/K}(\mathfrak{p}) = g}} \frac{1}{N(\mathfrak{p})^s} = \sum_{\substack{\mathfrak{p} \\ F_{L/K}(\mathfrak{p}) \in \varphi^{-1}(g)}} \frac{1}{N(\mathfrak{p})^s} + g(s).$$

Lemma 7.31 implies that the last sums equals

$$\frac{\#(\varphi^{-1}(g))}{[L:K]} \log \frac{1}{s-1} + g(s),$$

but obviously we have $\#(\varphi^{-1}(g)) = [L:M]$, and so

$$\sum_{\substack{\mathfrak{p} \\ F_{M/K}(\mathfrak{p}) = g}} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{[M:K]} \log \frac{1}{s-1} + g(s). \qquad \square$$

Corollary. *Theorem 7.30* holds for all Abelian extensions of the rationals.*

Proof : Apply Theorem 6.18 and the lemma. □

Lemma 7.33. *If Theorem 7.30, or 7.30*, is true for all cyclic extensions of every algebraic number field, then it is true for all normal extensions.*

Proof : Let L/K be normal, and select an arbitrary element $g \in Gal(L/K)$. We consider the set P_g of all prime ideals $\mathfrak{p}$ of R_K which do not ramify in L/K, and for which $F_{L/K}(\mathfrak{p})$ is the conjugacy class containing g. For $\mathfrak{p} \in P_g$ let $\mathfrak{P} \in R_L$ be the prime ideal lying over $\mathfrak{p}$ with

$$\left[\frac{L/K}{\mathfrak{P}}\right] = g. \tag{7.28}$$

Let $Z(g)$ be the centralizer of g (i.e., the set of all elements of $Gal(L/K)$ commuting with g), $C(g)$ the cyclic group generated by g, and $i(g)$ the index of $C(g)$ in $Z(g)$. Observe that $i(g)$ coincides with the number of those prime ideals $\mathfrak{P}$ over a given $\mathfrak{p} \in P_g$, satisfying (7.28), this number being independent of $\mathfrak{p}$. In fact, if $t \in Gal(L/K)$, and $\mathfrak{P}$ satisfies (7.28) then, by Proposition 7.28, the equality

$$\left[\frac{L/K}{t(\mathfrak{P})}\right] = g$$

holds if and only if $tgt^{-1} = g$, i.e., if and only if $t \in Z(g)$, and this shows that there are exactly $\#C(g)$ distinct prime ideals of the form $t(\mathfrak{P})$ (with $t \in Gal(L/K)$), since the decomposition group of $\mathfrak{P}$ equals $C(g)$.

Let M be the subfield of L corresponding to $C(g)$, and denote by $\mathfrak{q}$ the prime ideal of R_M lying below $\mathfrak{P}$, which is a fixed prime ideal over $\mathfrak{p}$ satisfying (7.28). Proposition 6.7 shows that $\mathfrak{q}R_L = \mathfrak{P}$ and $N_{M/K}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{P})$ (because of $f_{M/K}(\mathfrak{q}) = 1$), hence the conditions

$$g(x) \equiv x^{N(\mathfrak{q})} \pmod{\mathfrak{P}}$$

and

$$g(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

are equivalent. Thus $\left[\frac{L/M}{\mathfrak{P}}\right] = g$, and $F_{L/M}(\mathfrak{q}) = g$. We see that if $F_{L/K}(\mathfrak{p})$ is the conjugacy class containing g, then $\mathfrak{p}$ has $i(g)$ prime ideal divisors $\mathfrak{q}$ in R_M, satisfying $N_{M/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{p})$ and $F_{L/M}(\mathfrak{q}) = g$. Note that also conversely, if $F_{L/M}(\mathfrak{q}) = g$ and $N_{M/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{p})$, then $g \in F_{L/K}(\mathfrak{p})$, and the set of remaining prime ideals $\mathfrak{Q} \in R_M$ with $F_{L/M}(\mathfrak{Q}) = g$ is regular of density zero, since every such ideal is of degree > 1 over the rationals. We can thus write

$$i(g) \sum_{\substack{\mathfrak{p} \\ g \in F_{L/K}(\mathfrak{p})}} \frac{1}{N(\mathfrak{p})^s} = \sum_{\substack{\mathfrak{q} \\ F_{L/M}(\mathfrak{q}) = g}} \frac{1}{N(\mathfrak{q})^s} + g(s). \tag{7.29}$$

Now we use the assumed validity of Theorem 7.30 for all cyclic extension in the case of the extension L/M. This leads us to

$$\begin{aligned} \sum_{\substack{\mathfrak{q} \\ F_{L/M}(\mathfrak{q}) = g}} \frac{1}{N(\mathfrak{q})^s} &= \frac{1}{[L:M]} \log \frac{1}{s-1} + o\left(\log \frac{1}{s-1}\right) \\ &= \frac{1}{\#C(g)} \log \frac{1}{s-1} + o\left(\log \frac{1}{s-1}\right), \end{aligned}$$

and now (7.29) implies

$$\sum_{\substack{\mathfrak{p} \\ g \in F_{L/K}(\mathfrak{p})}} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{\#Z(g)} \log \frac{1}{s-1} + o\left(\log \frac{1}{s-1}\right),$$

and it suffices to recall that

$$\#Z(g) = \frac{\#Gal(L/K)}{\#\{tgt^{-1} : t \in Gal(L/K)\}} .$$

If we assume that Theorem 7.30* holds for all cyclic extensions, then in the argument above we can replace $o\left(\log \frac{1}{s-1}\right)$ by $g(s)$, yielding Theorem 7.30* for the extension L/K. □

So we are left with cyclic extensions. To deal with them a technical lemma is needed:

Lemma 7.34. *If L/K is a finite extension, and G is a finite Abelian group, then there exists a normal extension M/K with $Gal(M/K) \sim G$, which can be embedded in a cyclotomic extension N/K, and satisfies $L \cap M = K$.*

Proof : Let $G = \prod_{i=1}^{r} C_{p_i^{\alpha_i}}$ be the factorization of G into primary cyclic factors. For every set of distinct rational primes $q_1, \ldots, q_r$, not dividing $d(K)$, and satisfying

$$q_i \equiv 1 + p_i^{\alpha_i} \pmod{p_i{}^{\alpha_i+1}} \quad (i = 1, 2, \ldots, r)$$

put $m = q_1 \cdots q_r$ and $K_m = K(\zeta_m)$ (the existence of such primes q_i results from Corollary 7 to Theorem 7.25). Theorem 2.20 and Corollary to Theorem 4.26 show that all prime divisors of $d(\mathbb{Q}(\zeta_m))$ divide m, and so by Theorem 4.26 we obtain $[K_m : K] = \varphi(m)$. Since for relatively prime m_1, m_2 we have $K(\zeta_{m_1}, \zeta_{m_2}) = K_{m_1 m_2}$, we get

$$\begin{aligned}[K(\zeta_{m_1}, \zeta_{m_2}) : K] &= \varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2) \\ &= [K_{m_1} : K][K_{m_2} : K],\end{aligned}$$

hence $K_{m_1} \cap K_{m_2} = K$. This shows that if v is the number of subfields of L containing K, then from every system of $v+1$ fields K_{m_i} one can extract one, say $K_m = N$ with $N \cap L = K$. If $m = q_1 \cdots q_r$ and $q_i = 1 + b_i p_i^{\alpha_i}$ $(i = 1, 2, \ldots, r)$, then the Galois group $Gal(N/K)$ is isomorphic to

$$\prod_{i=1}^{r} C_{b_i p_i^{\alpha_i}} = \prod_{i=1}^{r} \left(C_{b_i} \times C_{p_i^{\alpha_i}} \right),$$

since $p_i \nmid b_i$. Now let M be the field, corresponding to the subgroup $\prod_{i=1}^{r} C_{b_i}$ of $Gal(N/K)$. Obviously $Gal(M/K) \sim G$ and $L \cap M = K$. □

Now, as all necessary preparations have been made, we can proceed with the proof of Theorem 7.30. Let L/K be a cyclic extension with Galois group G, and let M/K be a normal extension contained in a suitable cyclotomic

extension, and satisfying $L \cap M = K$. Lemma 7.34 assures the existence of such extension, and permits us to choose freely the Abelian Galois group $G_1 = Gal(M/K)$. Fix an element $g \in G$, and let f be its order. Leaving for a while aside the final choice of G_1, assume now only that G_1 contains an element t of order f_t divisible by f. Let U be the cyclic subgroup of the group $G \times G_1 \sim Gal(LM/K)$ generated by the pair (g,t), and denote by N the subfield of LM, corresponding to U. The extension LM/N is cyclic with Galois group U, and MN/N is also cyclic with Galois group $U/(gp(g) \cap U) \sim gp(t)$, where $gp(x)$ denotes the cyclic group generated by x. Note that MN is contained in a cyclotomic extension of N. Lemma 7.32 implies that if $\bar{t}$ is the coset in $U/(gp(g) \cap U)$ determined by t, then

$$\sum_{\substack{\mathfrak{q} \\ F_{MN/N}(\mathfrak{q})=\bar{t}}} \frac{1}{N(\mathfrak{q})^s} = \frac{1}{f_t} \log \frac{1}{s-1} + g(s). \tag{7.30}$$

Now let $\mathfrak{q}$ be a prime ideal in R_N of first degree over K, and let $\mathfrak{p}$ be the prime ideal of R_K lying below it. By Theorem 7.29 (iv) we have $F_{MN/N}(\mathfrak{q}) = F_{M/K}(\mathfrak{p})$, and thus (7.30) implies

$$\begin{aligned} \sum_{\substack{\mathfrak{p} \text{ splits in } N \\ F_{M/K}(\mathfrak{p})=t}} \frac{1}{N(\mathfrak{p})^s} &= \frac{1}{[N:K]} \sum_{\substack{\mathfrak{q} \\ F_{MN/N}(\mathfrak{q})=\bar{t}}} \frac{1}{N(\mathfrak{q})^s} \\ &= \frac{1}{f_t[N:K]} \log \frac{1}{s-1} + g(s). \end{aligned} \tag{7.31}$$

Because of $Gal(N/K) \sim G/U$, Corollary 1 to Theorem 7.29 implies that a prime ideal $\mathfrak{p}$ of R_K splits in N/K if and only if $F_{L/K}(\mathfrak{p}) \in U$. Hence the set

$$A_t = \{\mathfrak{p} \subset R_K : \ F_{M/K}(\mathfrak{p}) = t, \ \mathfrak{p} \text{ splits in } N/K\}$$

coincides with

$$\{\mathfrak{p} \subset R_K : \ F_{M/K}(\mathfrak{p}) = t, F_{LM/K}(\mathfrak{p}) = (gt)^r \text{ for some } r\}.$$

Now Theorem 7.29 (iii) shows that the condition $F_{LM/K}(\mathfrak{p}) = (gt)^r$ is equivalent to the conjunction of $F_{L/K}(\mathfrak{p}) = g^r$ and $F_{M/K}(\mathfrak{p}) = t^r$, thus for $\mathfrak{p} \in A_t$ we must have $t^r = t$, i.e. $r \equiv 1 \pmod{f_t}$, and also $r \equiv 1 \pmod{f}$, because $f | f_t$. Finally we arrive at

$$A_t = \{\mathfrak{p} \subset R_K : \ F_{M/K}(\mathfrak{p}) = t, F_{L/K}(\mathfrak{p}) = g\},$$

and (7.31) leads to

$$\sum_{\substack{F_{L/K}(\mathfrak{p})=g \\ F_{M/K}(\mathfrak{p})=t}} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{f_t[N:K]} \log \frac{1}{s-1} + g(s). \tag{7.32}$$

Denote by $C(f)$ the number of $t \in G_1$ whose orders are divisible by f, and add the equalities (7.32) for all such t's. In view of

$$f_t[N:K] \le [LM:N][N:K] = [LM:K]$$

this gives

$$\sum_{F_{L/K}(\mathfrak{p})=g} \frac{1}{N(\mathfrak{p})^s} \ge \frac{C(f)}{[LM:K]} \log \frac{1}{s-1} + O(1)$$

as s tends to 1 over real numbers exceeding 1.

It is now time to choose the group G_1. We shall do it in such a way that the ratio $C(f)/\#G_1$ falls between $1-\epsilon$ and 1, where ϵ is an arbitrary fixed positive number. To show that such choice is possible, factorize $f = p_1^{a_1} \cdots p_r^{a_r}$, and note that if G_1 is a cyclic group of order $p_1^{b_1} \cdots p_r^{b_r}$, where $b_i \ge a_i$ $(i = 1, 2, \ldots, r)$, then G_1 contains

$$\prod_{i=1}^{r} \left(p_i^{b_i} - p_i^{a_i - 1} \right)$$

elements of orders divisible by f, and so for such group the ratio $C(f)/\#G_1$ equals

$$\prod_{i=1}^{r} \left(1 - p_i^{a_i - b_i - 1} \right),$$

and thus can be made arbitrarily close to 1 by a suitable choice of the b_i's. Therefore for $s > 1$ we have

$$\sum_{F_{L/K}(\mathfrak{p})=g} \frac{1}{N(\mathfrak{p})^s} \ge \left(\frac{1}{[L:K]} + o(1) \right) \log \frac{1}{s-1}, \tag{7.33}$$

and adding the resulting equalities for $g \in G$ we get

$$\log \frac{1}{s-1} + O(1) = \sum_{g \in G} \sum_{F_{L/K}(\mathfrak{p})=g} \frac{1}{N(\mathfrak{p})^s} \ge (1 + o(1)) \log \frac{1}{s-1},$$

which is possible only if in (7.33) the equality sign occurs. □

Thus the proof of Theorem 7.30 is complete. Now we deduce the stronger Theorem 7.30* from Artin's reciprocity law. First we have to state the latter. There are several formulations of this theorem, which is fundamental for the class-field theory. We choose the version which is most suitable for our purpose.

Artin's Reciprocity Law. *If L/K is Abelian with Galois group G, then there exists an ideal $\mathfrak{f}$ in R_K such that the set of prime ideals ramified in L/K coincides with the set of prime ideals dividing $\mathfrak{f}$. Moreover, if $\mathfrak{p}_1$, $\mathfrak{p}_2$ are two unramified prime ideals lying in the same class in $H_{\mathfrak{f}}^*(K)$, then $F_{L/K}(\mathfrak{p}_1) =$*

$F_{L/K}(\mathfrak{p}_2)$, and the map $H_{\mathfrak{f}}^*(K) \longrightarrow G$, induced in this way by $F_{L/K}$ is a surjective homomorphism.

Theorem 7.30* is an immediate corollary. Indeed, in view of Lemma 7.33 it suffices to deal with the case of cyclic L/K, and the reciprocity law shows that the set of all prime ideals $\mathfrak{p}$ in R_K, for which $F_{L/K}(\mathfrak{p})$ is a given element $g \in Gal(L/K)$, is non-void, and consists of all prime ideals lying in certain classes of $H_{\mathfrak{f}}^*(K)$, the number of these classes being independent of g. It remains to apply Corollary 6 to Proposition 7.16. □

Now we turn to applications of Chebotarev's Density Theorem. We start with two old results of Frobenius and Kronecker, which formed the first steps towards Theorem 7.30.

Proposition 7.35. *(i) Let L/K is normal of degree n. If for a given $g \in Gal(L/K)$ we denote by $A(g)$ the union of conjugacy classes of $g, g^2, \ldots$, then the set of all prime ideals $\mathfrak{p}$ of R_K satisfying $F_{L/K}(\mathfrak{p}) \in A(g)$ is infinite, and its Dirichlet density equals $\#A(g)/n$.*

(ii) If $[L : K] = n$ and for $m = 0, 1, \ldots, n$ we denote by P_m the set of all prime ideals of R_K having exactly m prime ideal divisors of degree one in R_L, then every set P_m has a Dirichlet density, say d_m, and one has

$$\sum_{j=0}^{n} d_j = \sum_{j=1}^{n} j d_j = 1.$$

Proof : Assertion (i) results immediately from Theorem 7.30, since every set $A(g)$ is a union of disjoint conjugacy classes.

To prove (ii) observe that the existence of the densities d_m is a consequence of Corollary 3 to Theorem 7.29 and Theorem 7.30. Since the sets P_m are disjoint, and their union contains every prime ideal of R_K we get $d_0 + d_1 + \cdots + d_n = 1$. To obtain the second equality we use Corollary 3 to Proposition 7.16, getting for $\sigma > 1$

$$\begin{aligned}
(1 + o(1)) \log \frac{1}{s-1} &= \sum_{\substack{\mathfrak{P} \subset R_L \\ f_{L/K}(\mathfrak{P})=1}} \frac{1}{N(\mathfrak{P})^s} \\
&= \sum_{m=0}^{n} \sum_{\substack{\mathfrak{P} \\ f_{L/K}(\mathfrak{P})=1, \mathfrak{P} \cap R_K \in P_m}} \frac{1}{N(\mathfrak{P})^s} = \sum_{m=0}^{n} m \sum_{\mathfrak{p} \in P_m} \frac{1}{N(\mathfrak{p})^s} + g(s) \\
&= \left(\sum_{m=1}^{n} m d_m + o(1) \right) \log \frac{1}{s-1},
\end{aligned}$$

whence

$$\sum_{m=1}^{n} m d_m = 1. \qquad \square$$

Let L/K be finite of degree n, and let M/K be the smallest normal extension of K containing L. Denote by G the Galois group of M/K, let $L_1 = L, L_2, \ldots, L_n$ be the fields conjugated to L over K, and observe that G acts as a permutation group on the set of these fields. In the next proposition we keep this interpretation in mind.

Proposition 7.36. *The set of all prime ideals $\mathfrak{p}$ of R_K unramified in L/K, and satisfying*

$$\mathfrak{p}R_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r,$$

with fixed $f_i = f_{L/K}(\mathfrak{P}_i)$ $(i = 1, 2, \ldots, r)$ has a density, which equals the relative frequency in G of the set of all permutations which are products of r disjoint cycles of orders $f_1, f_2, \ldots, f_r$, respectively.

Proof : We need an auxiliary result:

Lemma 7.37. *If $\mathfrak{p}$ is a prime ideal of K unramified in L/K, $g \in F_{M/K}(\mathfrak{p})$, and $g = g_1 \cdots g_r$ is the factorization of g into disjoint cycles, then*

$$\mathfrak{p}R_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r,$$

with

$$f_{L/K}(\mathfrak{P}_i) = \#g_i \quad (i = 1, 2, \ldots, r).$$

Proof : Let U be the subgroup of G corresponding to L. Fix $1 \leq i \leq r$, let L_a be an element of the cycle g_i, choose $t_i \in G$, mapping L_a onto L_1, and consider $h_i = t_i g t_i^{-1}$. By Theorem 7.29 (v) there exists a prime ideal $\mathfrak{P}_i$ lying over $\mathfrak{p}$ with $f_{L/K}(\mathfrak{P}_i) = \#H_i/\#(H_i \cap U)$, where H_i is the subgroup generated by h_i. Observe that in the factorization of h_i into distinct cycles the field L_1 lies in a cycle of length $f_i = \#g_i$. Since the remaining cycles leave L_1 invariant, they must belong to U, and it follows that f_i is the smallest positive integer with $h_i^{f_i} \in U$. Therefore $f_{L/K}(\mathfrak{P}_i) = f_i$ results. Since for distinct i's we get distinct prime ideals $\mathfrak{P}_i$, we are ready. □

Proposition 7.36 follows immediately from the lemma and Theorem 7.30. □

4. Now we give an application of Theorem 7.30 to the question to what extent an extension L/K is determined by the set $P(L/K)$ of all unramified prime ideals of R_K having at least one prime ideal divisor of first degree on L/K. It is clear that if L_1 and L_2 are conjugated over K, then the sets $P(L_1/K)$ and $P(L_2/K)$ coincide, thus $P(L/K)$ can determine L only up to an isomorphism over K. However, even this may fail, as we shall see. Let us call an extension L/K a *Bauerian extension*, if for every extension M/K the inclusion $P(M/K) \subset P(L/K)$ implies that M contains a subfield isomorphic

to L over K. It is convenient at this point to consider two sets of prime ideals differing only in finite number of elements as identical, since this allows us to forget about all ramified prime ideals. So in this subsection an inclusion $A \subset B$ for sets of prime ideals will mean that the difference $A \setminus B$ is finite, and an equality $A = B$ will mean that the symmetric difference of A and B is finite. The solution to our problem is given by the following theorem:

Theorem 7.38. *Let L/K and M/K be finite extensions, and let N/K be the minimal normal extension of K containing L. Denote by H and U the subgroups of $Gal(N/K)$ corresponding to L and $M \cap N$, respectively, and let $H_1 = H, H_2, \ldots, H_r$ be the subgroups of $Gal(N/K)$ conjugated to H. Then one has*

$$P(M/K) \subset P(L/K)$$

if and only if

$$U \subset \hat{H} = \bigcup_{i=1}^{r} H_i$$

holds.

Proof : We start with a lemma:

Lemma 7.39. *Let L/K be normal with Galois group G, and let M/K be an arbitrary finite extension. Put $N = L \cap M$, and denote by U the subgroup of G corresponding to N. Moreover, let C be an arbitrary conjugacy class in G. Then there exist infinitely many prime ideals $\mathfrak{p}$ in R_K having at least one prime ideal divisor of the first degree in M/K, and satisfying $F_{L/K}(\mathfrak{p}) = C$ if and only if the intersection $C \cap U$ is non-empty.*

If in addition N/K is normal, then this condition may be written in the form $C \subset U$.

Proof : Denote by R/K the minimal normal extension of K containing M. If U' is the subgroup of $Gal(R/K)$ corresponding to M, and $\mathfrak{P}$ is a prime ideal of R_R unramified in R/K, then the conditions

$$\left[\frac{R/K}{\mathfrak{P}}\right] \in U'$$

and $f_{M/K}(\mathfrak{P}') = 1$ (where $\mathfrak{P}'$ is the prime ideal of R_M below $\mathfrak{P}$) are equivalent by Theorem 7.29 (v). Thus a prime ideal $\mathfrak{p} \in R_K$ lies in $P(M/K)$ if and only if the intersection $F_{R/K}(\mathfrak{p}) \cap U'$ is non-void. If S is the composite of L and R, then $Gal(S/K)$ can be considered as the subgroup of the product $G \times Gal(R/K)$, consisting of all pairs (g_1, g_2) for which the restrictions of g_1 and g_2 to $L \cap R$ coincide. Observe now that if C_1 and C_2 are conjugacy classes in G and $Gal(R/K)$, respectively, then there exists a prime ideal $\mathfrak{p}$ with $F_{L/K}(\mathfrak{p}) = C_1$, $F_{R/K}(\mathfrak{p}) = C_2$ if and only if to every $g_2 \in C_2$ one can

select $g_1 \in C_1$ so that $g_1 g_2 \in Gal(S/K)$. Indeed, if $g_1 g_2$ lies in $Gal(S/K)$, then by Theorem 7.30 there exist infinitely many $\mathfrak{p}$ with $g_1 g_2 \in F_{S/K}(\mathfrak{p})$, and Theorem 7.29 (iii) implies $g_1 \in F_{L/K}(\mathfrak{p})$ and $g_2 \in F_{R/K}(\mathfrak{p})$. Conversely, if such $\mathfrak{p}$ exists, then by Theorem 7.29 (ii) the restrictions of C_1 and C_2 to $L \cap R$ coincide, being both equal to $F_{L\cap R/K}(\mathfrak{p})$, and our assertion becomes obvious.

Thus we see that one has $\mathfrak{p} \in P(M/K)$ if and only if the intersection $CU' \cap Gal(S/K)$ is not void. Since $Gal(S/K) \cap GU' = Gal(S/M)$ we see that the set of all $g_1 \in G$ for which there exists $g_2 \in U'$ such that $g_1 g_2 \in Gal(S/K)$ equals the restriction of $Gal(S/M)$ to L, which in turn coincides with $Gal(L/N) = U$, and so finally we find that the set

$$P(M/K) \cap \{\mathfrak{p} : \ F_{L/K}(\mathfrak{p}) = C\}$$

is non-empty if and only if there is $g_1 \in C$ lying in U, i.e., $C \cap U \neq \emptyset$.

If N/K is normal, then U is a normal subgroup of G, and then the conditions $C \cap U \neq \emptyset$ and $C \subset U$ are equivalent. □

To prove the theorem assume first that $P(M/K) \subset P(L/K)$. Let C be a conjugacy class in $Gal(N/K)$ which has elements in common with U. By Lemma 7.39 the set

$$\{\mathfrak{p} : \ F_{N/K}(\mathfrak{p}) = C, \mathfrak{p} \in P(M/K)\}$$

is infinite, and our assumption implies that the same holds for the set

$$\{\mathfrak{p} : \ F_{N/K}(\mathfrak{p}) = C, \mathfrak{p} \in P(L/K)\},$$

whence Lemma 7.39 leads to $C \cap H \neq \emptyset$. Now, if g lies in U, then one of its conjugates lies in H, hence $g \in \hat{H}$, proving $U \subset \hat{H}$.

To prove the converse assume $U \subset \hat{H}$. Then all subgroups conjugated with U are contained in $\hat{H}$, but for every $\mathfrak{p} \in P(M/K)$ the union of all subgroups conjugated with U contains $F_{N/K}(\mathfrak{p})$. This shows that $F_{N/K}(\mathfrak{p}) \cap H$ is non-void, proving $\mathfrak{p} \in P(L/K)$. □

Corollary 1. *If L/K is normal, then for every extension M/K the conditions $L \subset M$ and $P(M/K) \subset P(L/K)$ are equivalent, i.e., L/K is Bauerian.*

Proof : If $L \subset M$, then the multiplicativity of prime ideal degrees leads to $P(M/K) \subset P(L/K)$. Conversely, if $P(M/K) \subset P(L/K)$, then we apply the theorem just proved with $N = L$, $H = \{1\}$, thus $U = \{1\}$, $L \cap M = L$, and so $L \subset M$. □

Corollary 2. *Let L/K be a finite extension, and let M/K be the minimal normal extension of K containing L. Denote by H the subgroup of $Gal(M/K)$*

corresponding to L, and let $H_1 = H, H_2, \ldots, H_r$ be the subgroups conjugated with H. Then L/K is Bauerian if and only if for every subgroup U of $Gal(M/K)$ the condition $U \subset \bigcup_{i=1}^{r} H_i$ implies $U \subset H_i$ for a certain i.

Proof : Immediate from Theorem 7.38 and the definition of a Bauerian extension. □

The last corollary permits us to present an example of a non-Bauerian extension. Let $K = \mathbb{Q}$, and let $L = \mathbb{Q}(a)$, where a is a root of the polynomial $2X^5 - 32X + 1$, whose splitting field has the symmetric group on 5 letters for Galois group. The subgroup H corresponding to L consists of all permutations fixing a certain letter, say 1, thus for $i = 1, 2, \ldots, 5$ the group H_i consists of all permutations fixing i. If we now take

$$U = \{e, (123), (132), (12)(45)\},$$

then U is contained in the union of the groups H_i without being a subset of one of them. Thus the extension $L/\mathbb{Q}$ is not Bauerian.

5. Our next application concerns power residues. Let p be an arbitrary rational prime, and let K be an algebraic number field containing all p-th roots of unity. We shall call a set $A = \{a_1, \ldots, a_m\}$ of non-zero elements of K *p-independent* if the product

$$a_1^{x_1} \cdots a_m^{x_m}$$

with rational integral $x_1, \ldots, x_m$ can be a p-th power of an element of K only in the case when all exponents x_i are divisible by p. Equivalently, A is p-independent if its image in $K^*/(K^*)^p$, treated as a linear space over $\mathbb{F}_p$, is linearly independent.

Let $\mathfrak{q}$ be a prime ideal in R_K which does not divide pR_K, and is of degree one over $\mathbb{Q}$. Then its norm in $\mathbb{Q}(\zeta_p)$ is a prime ideal of degree one over $\mathbb{Q}$, and thus $q = N_{K/\mathbb{Q}}(\mathfrak{q})$ is a rational prime congruent to unity mod p by Theorem 4.40. Note also that $\mathfrak{q}$ is unramified in $K/\mathbb{Q}$.

For such $\mathfrak{q}$ and a non-zero element $a \in R_K$ one defines the p-th power residue symbol

$$\left(\frac{a}{\mathfrak{q}}\right)_p$$

as that p-th root of unity which is congruent to $a^{(q-1)/p} \pmod{\mathfrak{q}}$. This definition makes sense since the relation

$$a^{q-1} - 1 = \prod_{j=0}^{p-1} \left(a^{(q-1)/p} - \zeta_p^j\right) \equiv 0 \pmod{\mathfrak{q}}$$

shows that $a^{(q-1)/p}$ is congruent to a certain p-th root of unity, and indeed only to one of them, since they are distinct mod $\mathfrak{q}$, $\mathfrak{q}$ being unramified.

Theorem 7.40. *Let p be a fixed rational prime, and let K be an algebraic number field containing all p-th roots of unity. Let $a_1, \ldots, a_m \in R_K$ be given, forming a p-independent set, and let $z_1, \ldots, z_m$ be given p-th roots of unity.*

Then there exist infinitely many unramified prime ideals $\mathfrak{q}$ of degree one over $\mathbb{Q}$ with

$$\left(\frac{a_i}{\mathfrak{q}}\right)_p = z_i$$

for $i = 1, 2, \ldots, m$.

Proof : For $i = 1, 2, \ldots, m$ write $z_i = \zeta_p^{\epsilon_i}$ with $0 \leq \epsilon_i \leq p-1$, and put $\vartheta_i = a_i^{1/p}$ and $K_i = K(\vartheta_i)$. The extension K_i/K is normal with the cyclic group of p elements as Galois group. Let t_i be a generator of it acting on ϑ_i by $t_i(\vartheta_i) = \zeta_p \vartheta_i$. If $\mathfrak{q}$ is an unramified prime ideal of R_K of degree 1, then the definition of the Frobenius automorphism shows that the equality $F_{K_i/K}(\mathfrak{q}) = t_i^j$ is equivalent to $\left(\frac{a_i}{\mathfrak{q}}\right)_p = \zeta_p^j$. In fact, if $q = N(\mathfrak{q})$, then $F_{K_i/K}(\mathfrak{q}) = t_i^j$ holds if and only if

$$\zeta_p^j \vartheta_i \equiv \vartheta_i^q \pmod{\mathfrak{q}},$$

and this is in turn equivalent to

$$\zeta_p^j \equiv \vartheta_i^{q-1} \equiv a_i^{(q-1)/p} \pmod{\mathfrak{q}},$$

i.e., to

$$\left(\frac{a_i}{\mathfrak{q}}\right)_p = \zeta_p^j.$$

Observe now that it suffices to establish the equality $[L : K] = p^m$ for $L = K(\vartheta_1, \ldots, \vartheta_m)$, since then the set of all prime ideals satisfying the assertion of our theorem coincides with the set of all those unramified prime ideals $\mathfrak{q}$ of degree 1 for which

$$F_{L/K}(\mathfrak{q}) = [t_1^{\epsilon_1}, \ldots, t_m^{\epsilon_m}] \in \prod_{j=1}^{m} Gal(K(\vartheta_j)/K) = Gal(L/K),$$

and this set is infinite by Theorem 7.30. We will obtain this result as a special case of the following lemma:

Lemma 7.41. *Let p be a rational prime, and let K be a field of characteristic zero.*

(i) If $\gamma \in K$, and the polynomial $f(X) = X^p - \gamma$ is reducible over K, then γ is a p-th power of an element of K.

(ii) If a_1, a_2 are elements of K such that the fields $K(a_1^{1/p})$ and $K(a_2^{1/p})$ coincide (here $a^{1/p}$ denotes a solution of the equation $x^p = a$), then there is an element $b \in K$, and a rational integer r with $1 \leq r \leq p-1$, such that $a_1 = b^p a_2^r$.

(iii) If $a_1, \dots, a_m$ are p-independent elements of K then

$$[K(a_1^{1/p}, \dots, a_m^{1/p}) : K] = p^m.$$

Proof : (i) If $p = 2$ then the assertion is evident, so assume that p is an odd prime, and let ϑ be a fixed p-th root of γ, so that

$$f(X) = \prod_{j=0}^{p-1} (X - \zeta_p^j \vartheta).$$

Assume now that f is reducible over K. Then f has a factor of the form

$$g(X) = \prod_{j \in A} (X - \zeta_p^j \vartheta) \in K[X],$$

where A is a subset of $\{0, 1, \dots, p-1\}$ having $1 \leq r \leq p-1$ elements. If $R = \sum_{j \in A} j$, then $\zeta_p^R \vartheta^r = f(0) \in K$. Denote by λ the minimal positive rational integer for which with some $\alpha \in \mathbb{Z}$ we have

$$\zeta_p^\alpha \vartheta^\lambda \in K.$$

Writing $p = a\lambda + b$ with $a, b \in \mathbb{Z}$, $0 \leq b \leq \lambda - 1$ we obtain

$$\vartheta^p = (\vartheta^\lambda)^a \vartheta^b,$$

and thus $\zeta_p^{-a\alpha} \vartheta^b \in K$, which is possible only in the case $b = 0$. Hence λ divides p, thus either $\lambda = 1$, or $\lambda = p$.

If $\lambda = 1$, then $\xi = \zeta_p^\alpha \vartheta \in K$ is a root of g, hence also of f, so $\xi^p = \gamma$, as asserted. If $\lambda = p$ then in view of $p = \lambda \leq r \leq p-1$, we have a contradiction.

(ii) If $p = 2$, or one of the a_i's is a p-th power in K, then the assertion is obvious, so assume that this is not the case.

Let $L = K(a_1^{1/p}) = K(a_2^{1/p})$, and put $M_0 = K(\zeta_p), M = M_0(a_1^{1/p}) = L(\zeta_p)$. The extension M/M_0 is generated by a root of $X^p - a_1$, so either $a_1^{1/p} \in M_0$, or M/M_0 is cyclic of degree p. In the first case we would have

$$p = \deg_K a_1^{1/p} \leq \deg_K \zeta_p \leq p - 1,$$

a contradiction. Therefore only the second case has to be considered.

Write

$$a_2^{1/p} = \sum_{j=0}^{p-1} \lambda_j a_1^{j/p}$$

with $\lambda_j \in M_0$, and let g be that automorphism of M/M_0 which maps $a_1^{1/p}$ onto $\zeta_p a_1^{1/p}$. Then for a certain r with $1 \leq r \leq p-1$ we must have $g(a_2^{1/p}) = \zeta_p^r a_2^{1/p}$. But then

$$\sum_{j=0}^{p-1} \lambda_j \zeta_p^j a_1^{1/p} = \sum_{j=0}^{p-1} \lambda_j g(a_1^{j/p}) = g(a_2^{1/p}) = \zeta_p^r a_2^{1/p} = \sum_{j=0}^{p-1} \lambda_j \zeta_p^r a_1^{1/p},$$

hence we must have $\lambda_j = 0$ for $j \neq r$. This gives $a_2^{1/p} = \lambda_r a_1^{1/p}$ and $a_2 = \lambda_r^p a_1^r$. Since λ_r^p lies in K, we have either $\zeta_p^s \lambda_r \in K$ for a certain s, or the degree of λ_r over K equals p, but this is impossible in view of $[M_0 : K] \leq p-1$, and so we arrive at our assertion.

(iii) Write $K_0 = K$ and $K_{j+1} = K_j(a_{j+1}^{1/p})$ for $j = 0, 1, \ldots, m-1$. Observe that it suffices to show that the extensions K_{j+1}/K_j are all of degree p. If this were false for a certain j, then by (i) the element $c = a_{j+1}^{1/p}$ would lie in K_j. Let t be the minimal index for which $c \in K_t$. In view of $t \geq 1$ we have $K_t = K_{t-1}(c)$, and (ii) gives $a_{j+1} = \lambda^p a_j^r$ for a certain $\lambda \in K_{t-1}$ and $1 \leq r \leq p-1$. Note that λ^p lies in K. Let t_1 be the minimal index for which $\lambda \in K_{t_1}$. If $t_1 = 0$ then $\lambda \in K$, contradicting the p-independence of the a_i's. Thus $t_1 \geq 1$, hence $K_{t_1} = K_{t_1-1}(a_{t_1}^{1/p})$, and again we get $\lambda^p = \lambda_1^p a_{t_1}^{r_1}$ for a certain $\lambda_1 \in K_{t_1-1}$ and $0 \leq r_1 \leq p-1$, thus $a_{j+1} = \lambda_1^p a_{t_1}^{r_1} a_t^r$. Proceeding in this way we finally arrive at

$$a_{j+1} = \lambda_z a_t^r a_{t_1}^{r_1} \cdots a_{t_z}^{r_z}$$

with $\lambda_z \in K$, and not all exponents r_i divisible by p, contradicting the p-independence of the a_i's. □

The theorem follows now immediately. □

Corollary. *Let p be a rational prime, and K an algebraic number field. Then the equality $I_0^p = I_0 \cap I_K^p$ holds, i.e., every element of K^* which is a p-th power in every completion of K is a p-th power in K^*.*

Proof : Let $\langle x_v \rangle \in I_0 \cap I_K^p$. Then $x_v = x \in K^*$, and $x = y_v^p$ holds for every v with a certain $y_v \in K_v$. Multiplying x, if necessary, by a suitable p-th power we may assume that x lies in R_K. Now let $\mathfrak{q}$ be a prime ideal in R_K not containing x, and having degree 1 over $\mathbb{Q}$. Then with a suitable $y_\mathfrak{q} \in R_K$ the congruence $x \equiv y_\mathfrak{q}^p \pmod{\mathfrak{q}}$ holds. This implies

$$\left(\frac{x}{\mathfrak{q}}\right)_p \equiv x^{(N(\mathfrak{q})-1)/p} \equiv y_\mathfrak{q}^{N(\mathfrak{q})-1} \equiv 1 \pmod{\mathfrak{q}},$$

and thus

$$\left(\frac{x}{\mathfrak{q}}\right)_p = 1$$

holds for almost all prime ideals $\mathfrak{q}$ of degree 1 over $\mathbb{Q}$. By the last theorem this can happen only if the set $\{x\}$ is not p-independent, but this means that x is a p-th power in K^*. □

6. Our final application concerns the structure of R_L as an R_K-module for an extension L/K of degree n.

In the case $K = \mathbb{Q}$ the description is simple, as then R_L is a free $\mathbb{Z}$-module with n free generators, and by Theorem 1.32 the same happens if $h(K) = 1$. In the general case this theorem shows that R_L is isomorphic, as an R_K-module, to $R_K^{n-1} \oplus I$, where I is an ideal of R_K. Thus by Theorem 1.39 the isomorphism type of R_L is determined by n and the class of I in $H(K)$. This ideal class is denoted by $C_K(L)$, and called the *Steinitz class* of L/K. We shall now describe it in terms of the discriminant $\partial(L/K)$, and this will allow us to answer the question, when R_L is a free R_K-module.

To state the theorem we first define a homomorphism of $I_K^2 I_0/U_K^2$ onto the class-group $H(K)$. Denote by t the isomorphism of I_K/I_0U_K onto $I_K^2/I_0^2U_K^2$ induced by the map $a \mapsto a^2$ in I_K, and let t_1 be the surjective homomorphism of $I_K^2 I_0/U_K^2$ onto $I_K^2 I_0/U_K^2 I_0$ induced by $\langle x_v \rangle \mapsto \langle x_v \rangle \bmod I_0$. Moreover, define a homomorphism $v_0 : I_K^2 \longrightarrow I_K^2/I_0^2$ putting for $\xi = \langle x_v^2 y \rangle \in I_K^2 I_0$

$$v_0(\xi) = \langle x_v^2 \rangle \mod I_0^2.$$

This is well-defined because if $\langle x_v^2 y \rangle = \langle X_v^2 Y \rangle$ with $\langle x_v \rangle, X_v \rangle \in I_K$ and $\langle y \rangle, \langle Y \rangle \in I_0$, then by Corollary to Theorem 7.40 one has

$$\langle x_v^2 X_v^2 \rangle = \langle Y y^{-1} \rangle \in I_K^2 \cap I_0 = I_0^2,$$

thus the class $\langle x_v^2 \rangle \mod I_0^2$ is determined by ξ in a unique way. Because of $\operatorname{Ker} v_0 = I_0$ the map v_0 induces an isomorphism of $I_K^2 I_0/I_0$ onto I_K^2/I_0^2. Finally observe that v_0 induces a homomorphism of $I_K^2 I_0/U_K^2 I_0$ onto $I_K^2/U_K^2 I_0^2$, which we shall denote by u_0.

Let now u be the homomorphism of $I_K^2 I_0/U_K^2$ onto $H(K)$ obtained by the composition of the following maps:

$$I_K^2 I_0/U_K^2 \xrightarrow{t_1} I_K^2 I_0/U_K^2 I_0 \xrightarrow{u_0} I_K^2/U_K^2 I_0^2 \xrightarrow{t^{-1}} I_K/U_K I_0 \xrightarrow{t_2} H(K),$$

where t_2 denotes the natural homomorphism.

Having defined the map u we may now state the principal result of this subsection.

Theorem 7.42. *For every finite extension L/K of algebraic number fields we have*

$$C_K(L) = u(\partial(L/K)),$$

and if $\partial(L/K) = aI^2U_K^2$ $(a \in I_0,\ I \in I_K)$, then $C_K(L)$ is the class in $H(K)$ containing the ideal induced by the idele I.

Proof : Let M be a torsion-free and finitely generated R_K-module, and denote by V the linear K-space spanned by M. Put $n = \dim_K V$, and let N be a torsion-free R_K-module spanning the same space V. If v is a non-Archimedean valuation of K, then we can consider the R_v-modules M_v and

N_v generated by M and N, respectively, in the n-dimensional K_v-space $V_v = V \otimes_K K_v$. Since R_v is a principal ideal domain the resulting modules are free, and so there is an automorphism of V_v mapping N_v onto M_v. Denote by d_v the determinant of that automorphism, and observe that it is determined by M and N up to a unit factor from R_v. It follows that the ideal in R_v generated by d_v is determined uniquely by M and N. Let us denote this ideal by $[N : M]_v$.

Lemma 7.43. *If M, N, S are finitely generated torsion-free R_K-modules spanning the same linear K-space, and v is a non-Archimedean valuation of K, then*

(i) $[M : M]_v = R_v$,

(ii) $[M : N]_v[N : S]_v = [M : S]_v$,

(iii) The inclusion $M_v \subset N_v$ *implies* $[N : M]_v \subset R_v$,

(iv) For almost all v *one has* $[M : N]_v = R_v$.

Proof : Assertions (i) and (ii) are immediate. To prove (iii) it suffices to observe that the elements of a free R_v-basis of M_v are linear combinations with coefficients from R_v of the elements of a similar basis of N_v, and this implies $d_v \in R_v$. To prove (iv) consider non-zero $a, b \in R_K$ with $aM \subset N$ and $bN \subset M$. Now (ii) and (iii) imply

$$[N : M]_v[M : aM]_v \subset R_v, \quad [M : N]_v[N : bN]_v \subset R_v.$$

It follows from the definition that $[M : aM]_v = a^n R_v$, $[N : bN]_v = b^n R_v$, thus for almost all v we have $[M : aM]_v = [N : bN]_v = R_v$. Hence for these v, $[M : N]_v \subset R_v$, and $[M : N]_v^{-1} = [N : M]_v \subset R_v$, implying $[M : N]_v$, as asserted. □

Part (iv) of that lemma implies that the product $\prod_v [M : N]_v$ is a fractional ideal of K. Let us denote it by $[M : N]$. Its main properties are given in the following lemma:

Lemma 7.44. *Under the assumptions of the preceding lemma we have:*

(i) $[M : M] = R_K$,

(ii) $[M : N][N : S] = [M : S]$,

(iii) If $M \subset N$ *then* $[N : M] \subset R_K$,

(iv) If M *and* N *are fractional ideals in* K *then* $[M : N] = M^{-1}N$.

Proof : Assertions (i)-(iii) follow immediately from Lemma 7.43. To prove (iv) observe that M_v and N_v are fractional ideals in K_v, and so the automorphism mapping N_v onto M_v has the form $x \mapsto a_v x$ for a certain $a_v \in K_v^*$. Therefore

we get $[M : N]_v = a_v R_v$, thus $[M : N]_v = N_v M_v^{-1}$, and (iv) results from the definition of $[M : N]$. □

Now let F_1, F_2 be two free R_K-modules spanning the same K-space V as M. By Lemma 7.17 (ii) we have $[F_1 : M] = [F_1 : F_2][F_2 : M]$. Since F_1, F_2 are free, there is an isomorphism of F_1 onto F_2 which can be extended to an automorphism f of V, and also, for every non-Archimedean v, to an automorphism f_v of the corresponding K_v-space V_v. Now note that the image of $d = \det f$ in K_v equals $\det f_v$, hence $[F_1 : F_2]_v = dR_v$, and we get $[F_1 : F_2] = dR_K$. We see thus that $[F_1 : M]$ and $[F_2 : M]$ lie in the same class of $H(K)$, and this class depends only on M. Denote it by $Cl(M)$.

Lemma 7.45. *(i) If I is a fractional ideal of K then $I \in Cl(I)$,*

(ii) $Cl(M_1 \oplus M_2) = Cl(M_1)Cl(M_2)$,

(iii) If $M = R_K^{n-1} \oplus I$ with an ideal I of R_K then $I \in Cl(M)$.

Proof : (i) In this case R_K is a free R_K-module spanning the same space as I, thus $[R_K : I] \in Cl(I)$, and it remains to observe that Lemma 7.45 (iv) implies $[R_K : I] = I$.

(ii) Let F_1, F_2 be free R_K-modules spanning the same spaces V_1, V_2 as M_1 and M_2, respectively. Then the free R_K-module $F_1 \oplus F_2$ spans the same space $V_1 \oplus V_2$ as $M_1 \oplus M_2$, and the corresponding fact is true also for $(F_1 \oplus F_2)_v$ and $(M_1 \oplus M_2)_v$. Moreover, if $(d_i)_v$ is the determinant of the automorphism of $(V_i)_v$ induced by $(F_i)_v \longrightarrow (M_i)_v$ $(i = 1, 2)$, then the determinant of the automorphism of $(V_1 \oplus V_2)_v$ induced by $(F_1 \oplus F_2)_v \longrightarrow (M_1 \oplus M_2)_v$ equals $(d_1)_v(d_2)_v$, which gives

$$[F_1 \oplus F_2, M_1 \oplus M_2] = [F_1, M_1]_v [F_2, M_2]_v,$$

and this implies (ii).

The assertion (iii) follows easily from (i) and (ii). □

We can now conclude the proof of our theorem. Let $a_1, \ldots, a_n$ be an arbitrary K-basis of L, and let $D \in K^*$ be its discriminant. Let M be the free R_K-module generated by this basis, and choose an idele $\langle x_v \rangle \in I_K$ representing the discriminant $\partial(L/K)$ (which is an element of I_K/U_K^2, and even, as the proof of Theorem 6.31 shows, of $I_K^2 I_0/U_K^2$). Now consider, for every non-Archimedean valuation v of K, a basis $\{b_j\}$ of the R_v-module $\bigoplus_{w \in E_v} R_w$, where E_v is the set of inequivalent extensions of v to L, and R_w is the ring of integers of L_w. Denote the discriminant of this basis by d_v. We can express the b_j's in terms of the a_i's, and let D_v be the determinant of the matrix involved. Then

$$d_v = D_v^2 D. \tag{7.34}$$

Now we apply the homomorphism u to $\partial(L/K)$ looking at the behaviour of $\xi = \langle d_v \rangle$. We have $t_1(\xi) = \xi \mod U_K^2 I_0$, but since D is principal, (7.34) implies $t_1(\xi) = \langle D_v^2 \rangle \mod U_K^2 I_0$. Applying u_0 we obtain $\langle D_v^2 \rangle \mod U_K^2 I_0^2$, and it remains to show that this element is carried into $C_K(L)$ by $t_2 \circ t^{-1}$. To this end observe that $[M : R_L]$ is the ideal induced by the idele $\langle D_v \rangle$, $C_K(L)$ is the class containing $[M : R_L]$, and the image of this class under t is the coset of $U_K^2 I_o^2$ in I_K^2 containing $\langle D_v^2 \rangle$. □

Corollary 1. *The ring R_L is a free R_K-module if and only if $u(\partial(L/K)) = 1$, i.e., if $\partial(L/K)$ has a representative in I_0.* □

The next corollary gives an explicit formulation of Theorem 6.31:

Corollary 2. *If C is the class in $H(K)$ containing $d(L/K)$, then $C = C_K(L)^2$.*

Proof : Note that C contains the ideal induced by any representative of $\partial(L/K)$, $C_K(L)$ contains the ideal induced by the idele $\langle D_v \rangle$, and apply (7.34). □

Corollary 3. *If the extension L/K has a relative integral basis, then the discriminant $d(L/K)$ is principal. In the case of odd $h(K)$ the converse implication holds.*

Proof : If L/K has a relative integral basis, then $C_K(L) = 1$, and so by Corollary 2 the discriminant $d(L/K)$ is principal. If $2 \nmid h(K)$ and $d(L/K)$ is principal, then the same corollary implies $C_K(L) = 1$. □

We know from Chap. 1 that if $h(K) \neq 1$, then there exist non-free finitely generated and torsion-free R_K-modules. We show now that for suitable L/K the rings R_L have this property.

Proposition 7.46. *If M is an arbitrary torsion-free and non-cyclic R_K-module with two generators, then there exists a quadratic extension L/K such that R_L is isomorphic to M as an R_K-module.*

Proof : We need a lemma describing explicitly the class $C_K(L)$ for quadratic L/K:

Lemma 7.47. *Let L/K be a quadratic extension, write $L = K(\sqrt{a})$ with $a \in R_K$, and let $aR_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}}$. For every prime ideal $\mathfrak{p}$ with even $a_\mathfrak{p}$ let $s_\mathfrak{p}$ be the maximal rational integer s such that $\mathfrak{p}^s$ divides $2R_K$, and the congruence*

$$x^2 \equiv a\pi_p^{-\alpha_\mathfrak{p}} \pmod{\mathfrak{p}^{2s}}$$

is solvable, where π_p is an element of $\mathfrak{p} \setminus \mathfrak{p}^2$. For remaining prime ideals $\mathfrak{p}$ put $s_\mathfrak{p} = 0$. Then the class $C_K(L)$ contains the ideal

$$2 \prod_{\mathfrak{p}} \mathfrak{p}^{-s_\mathfrak{p} - m_\mathfrak{p}},$$

where $m_\mathfrak{p}$ denotes the integral part of $a_\mathfrak{p}/2$.

Proof: Let us look at the components $\partial_v(L/K)$ of $\partial(L/K)$. If v is Archimedean, then

$$\partial_v(L/K) = \begin{cases} \operatorname{sgn} F_v(a) & \text{if } v \text{ is real,} \\ 1 & \text{if } v \text{ is complex,} \end{cases}$$

where F_v denotes the embedding of K in K_v, and if v is non-Archimedean then

$$\partial_v(L/K) = \begin{cases} 1 \bmod U^2(K_v) & \text{if } \mathfrak{p}_v \text{ splits in } L/K, \\ \partial(K_v(\sqrt{a})/K_v) & \text{otherwise.} \end{cases}$$

Consider now the case when the prime ideal $\mathfrak{p}$ corresponding to v does not split, fix $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, and write for shortness $m = m_\mathfrak{p}$, $s = s_\mathfrak{p}$ and $\alpha = \alpha_\mathfrak{p}$.

If $\mathfrak{p} \nmid 2a$, then Theorem 5.15 (i) gives

$$\partial_v(L/K) = a \bmod U^2(K_v) = (2\pi^{-m-s})^2 a \bmod U^2(K_v),$$

because in this case $m = s = 0$, and 2 is a unit in K_v.

If $\mathfrak{p} \nmid 2$ and $\alpha > 0$ is even, then writing $a = \epsilon(\pi^m)^2$ with $\epsilon \in U(K_v)$ one sees that $K_v(\sqrt{a}) = K_v(\sqrt{\epsilon})$. Theorem 5.15 (i) gives now

$$\partial_v(L/K) = \epsilon \bmod U^2(K_v) = (2\pi^{-m-s})^2 a \bmod U^2(K_v),$$

since again we have $s = 0$ and $2 \in U(K_v)$.

If α is odd then the distinction between the cases $\mathfrak{p}|2$ and $\mathfrak{p} \nmid 2$ is irrelevant. Writing $a = \epsilon\pi(\pi^m)^2$ with $\epsilon \in U(K_v)$ we get $K_v(\sqrt{a}) = K_v(\sqrt{\pi\epsilon})$, and applying Theorem 5.15 (ii) we arrive at

$$\partial_v(L/K) = 4\epsilon\pi \bmod U^2(K_v) = 4a(\pi^{-m-s})^2 \bmod U^2(K_v).$$

It remains the case $\mathfrak{p}|2$ and $2|\alpha$. Here $a = \epsilon\pi^{2m}$ ($\epsilon \in U(K_v)$), thus $K_v(\sqrt{a}) = K_v(\sqrt{\epsilon})$, and by Theorem 5.15 (iii) we get

$$\partial_v(L/K) = 4\epsilon\pi^{-2s} \bmod U^2(K_v) = a(2\pi^{-m-s})^2 \bmod U^2(K_v).$$

These results show that $\partial(L/K) = a\xi^2 \bmod U_K^2$, where $\xi = \langle x_v \rangle$ with

$$x_v = \begin{cases} 2\pi_v^{-s_\mathfrak{p} - m_\mathfrak{p}} & \text{if } v \text{ is non-Archimedean,} \\ 1 & \text{otherwise.} \end{cases}$$

Indeed, one has only examine the v-component for those v for which $\mathfrak{p} = \mathfrak{p}_v$ splits in L/K. If $\mathfrak{p} \nmid 2$ then $s_\mathfrak{p} = 0$ and a is a square in K_v, say $a = b^2$. Then $ax_v^2 = 4b^2\pi^{-m_\mathfrak{p}} \bmod U^2(K_v)$. Obviously $2b\pi^{-m}$ lies in $U(K_v)$, and so

$ax_v^2 = 1 \bmod U^2(K_v)$, hence $\partial_v(L/K) = ax_v^2 \bmod U^2(K_v)$. If $\mathfrak{p}|2$ then $a\pi^{-\alpha}$ is a square, say b^2, in K_v. Thus $\mathfrak{p}^s|2$ and $\mathfrak{p}^{s+1} \nmid 2$. Now

$$ax_v^2 = 4a(\pi^{-s-m})^2 \bmod U^2(K_v) = (2b\pi^{-s})^2 \bmod U^2(K_v) = 1 \bmod U^2(K_v),$$

as required.

Finally, observe that by Theorem 7.42 $C_K(L)$ coincides with $u(\partial(L/K))$, which equals the class in $H(K)$ containing the ideal induced by the idele ξ, and this ideal is equal

$$2\prod_{\mathfrak{p}} \mathfrak{p}^{-s_\mathfrak{p}-m_\mathfrak{p}}. \qquad \square$$

To prove the proposition it remains to show that to every class $C \in H(K)$ there exists a quadratic extension L/K with $C_K(L) = C$. To this end write

$$I = \prod_{\substack{\mathfrak{p} \\ 2 \in \mathfrak{p}}} \mathfrak{p},$$

and let $\mathfrak{q}_1 \in C^{-1}$ be a prime ideal not dividing I. Select a prime ideal $\mathfrak{q}_2$, not dividing $\mathfrak{q}_1 I$, for which the product $I\mathfrak{q}_1^2\mathfrak{q}_2$ is a principal ideal, generated by a, say. Now put $K = K(\sqrt{a})$. According to the lemma the class $C_K(L)$ contains the ideal

$$\prod_{\mathfrak{p}|aR_K} \mathfrak{p}^{-s_\mathfrak{p}-m_\mathfrak{p}},$$

and for $\mathfrak{p}$ dividing aR_K we have $s_\mathfrak{p} = m_\mathfrak{p} = 0$ with the single exception of $\mathfrak{p} = \mathfrak{q}_1$, in which case $s_\mathfrak{p} = 0$, $m_\mathfrak{p} = 1$. Hence $\mathfrak{q}_1^{-1}$ lies in $C_K(L)$, and we get $C = C_K(L)$. $\square$

Corollary. *The equality $h(K) = 1$ holds if and only if every quadratic extension of K has a relative integral basis.* $\square$

The last proposition shows that the Steinitz classes $C_K(L)$ cover $H(K)$ when L ranges over all quadratic extensions of K. An analogous result for normal extensions of a fixed odd degree fails to hold in general, as can be seen from the following result of McCulloh [66]:

Proposition 7.47. *Let N be an odd integer, and denote by T_N the greatest common divisor of numbers $(p-1)/2$, when p runs over all prime divisors of N. Assume that T_N has an odd prime divisor q, and choose a field K with $q|h(K)$. Then there is a class in $H(K)$ which is not the Steinitz class of any normal extension L/K of degree N.*

Proof: If L/K is normal of degree N, then by Corollary 1 to Proposition 6.9 we have $d(L/K) = I^{2T_N}$ with a certain ideal I of R_K. If X is the class of I

in $H(K)$, then by Corollary 2 to Lemma 7.45 we get $C_K(L)^2 = X^{2T_N}$. Since $q|(T_N, h(K))$ and q is odd, we see that $C_K(L)$ must be a q-th power, thus lies in a proper subgroup of $H(K)$. □

Note that in view of a result of Nagell [22], which we shall prove in the next chapter (see Theorem 8.25), one can take for K a suitable imaginary quadratic field.

7.4. Notes to Chapter 7

1. The first application of Dirichlet series to number theory was given by Dirichlet [37a,b], [38], [39]. He used the functions $L(s, \chi)$, which in our terminology are zeta-functions attached to Dirichlet characters. The first systematic use of $\zeta(s)$ was made by Riemann [60]. Dedekind's zeta-function was introduced in Dedekind [71], although in certain special cases it appeared already in Eisenstein [44b]. Dedekind established the existence of the limit $\lim_{s\to 1}(s-1)\zeta_K(s)$, and its connection with the class-number. Landau [03a] was the first to continue $\zeta_K(s)$ beyond the line Re $s = 1$ to the open half-plane Re $s > 1 - [K : \mathbb{Q}]^{-1}$. Hecke [17a] proved that Dedekind's zeta-function can be extended to a meromorphic function in the complex plane, and found the functional equation for this function (our Theorem 7.3). For some fields, including pure cubic and Abelian extensions of $\mathbb{Q}$ this has been known earlier (cf. Dedekind [00], Hurwitz [82]). Other proofs of Theorem 7.3 were given in Müntz [24], Siegel [22b] and Tate [50]. The proof given by us follows that of Tate. A version of Hecke's proof appears in Neukirch [92].

2. A simple product formula for the residue $h\kappa$ of $\zeta_K(s)$ was given in Wintner [46b] (see also P.Cassou-Noguès, Fresnel [79]). Corollary 4 to Theorem 7.3 was improved consecutively in Siegel [69a], Lavrik [70] and Lavrik, Edgorov [75]. Lavrik showed that one can take $(2/3)^n$ for the constant occurring in that corollary. For pure cubic fields the bound $h(K)R(K) \leq (\sqrt{D}\log D)/(6\sqrt{3})$ was obtained in Barrucand, Loxton, Williams [87], who removed the factor $\log\log D$ from a bound proved by H.Cohn [56b]. For explicit upper bounds for $h\kappa$ see also Hoffstein [79] and Louboutin [98b], [00]. A lower bound was given in Le [95] in the case of Abelian extensions with odd degree. For pure extensions of prime degree see Barrucand, Louboutin [93].

A discussion of various ways to generalize results about $\zeta(s)$ to $\zeta_K(s)$ was given in S.Lang [71].

3. Zeta-functions with arbitrary Hecke characters[3] were introduced by Hecke [18], who also proved Theorem 7.9. He utilized the language of ideal

[3] The name *Hecke character* appears first in Weil [74]. Hecke called them *Grössencharaktere*, i.e. *characters of magnitude*.

numbers. The modern approach is due to Weil [36], [51]. Cf. Hasse [54b], Tate [50]. Our proof of Theorem 7.9 is modelled upon Tate [50]. This method was independently found by Iwasawa, but not published (see Iwasawa [92]). For an interpretation of this result in terms of distributions see Weil [66].

The Hilbert-Ostrowski theorem (Ostrowski [20]) states that ζ_K and its derivatives form an algebraically independent set. Popken [66] proved that $\zeta_K(s)$ cannot satisfy an algebraic difference-differential equation, and studied also the algebraic independence of sets of Dedekind zeta-functions of quadratic fields over the ring of polynomials with complex coefficients (cf. Reich [82]). If $K_1, \ldots, K_m$ are distinct normal fields, then their Dedekind zeta-functions are linearly independent (Nicolae [00]), and Voronin [75b] established functional independence for finite families of Dirichlet L-functions.

It has been proved in Voronin [75a] that every regular function on the complex plane can be uniformly approximated by translations of Riemann's zeta-function, and the same holds for Dirichlet's L-functions (cf. Laurinčikas [96]). It turned out later that the same property have Dedekind's zeta functions (Reich [80], [82]) and zeta functions associated with Hecke characters (Mishou [01], [03]).

4. Corollary 5 to Theorem 7.3 is due to Perlis [77a]. Fields satisfying its assumptions are called *arithmetically equivalent* . The first examples of such fields (of degree 180) were constructed by Gassmann [26]. One says that a field K is *solitary*, if the only fields arithmetically equivalent to K are isomorphic to K. It has been shown by Perlis [77a] that every field of degree ≤ 6 is solitary, and later it turned out that also fields of degree 9 and 10 are solitary (Rzedowski-Caldéron, Villa-Salvador [96]), whereas there are non-solitary fields of degrees 7 and 8 (Perlis [77a]).

Arithmetically equivalent fields may have distinct class groups. Perlis, de Smit [94] showed that this happens for $\mathbb{Q}(\sqrt[8]{-15})$ and $\mathbb{Q}(\sqrt[8]{-240})$ (cf. de Smit [98]). Also the norm-sets $N_{K/\mathbb{Q}}(R_K)$ may be different (Coykendall [00]). Perlis [77b] proved that two fields K, L of odd prime degree p are arithmetically equivalent if and only if the degree of their composite is less than p^2. It follows from a conjecture of Wielandt (see Cameron [72]), which is now a theorem (see Th.1.51 in Gorenstein [82]), that there do not exist three pairwise non-isomorphic arithmetically equivalent fields of odd prime degree.

For further results concerning arithmetically equivalent fields see Jacobson, Vélez [90], Klingen [78], Komatsu [76c], [78], [84], Perlis [78], [85], Perlis, Schinzel [79], Stuart, Perlis [95]. For generalizations to relative extensions see Klingen [78], Nagata [86]. The theory of arithmetically equivalent fields is presented in the book of Klingen [98]. Another types of field equivalence were introduced in Somodi [02], and Sonn [85] (cf. Lochter [93]).

5. If $\chi(I) = \chi_1(I)N(I)^s$ is a Hecke character of conductor $\mathfrak{f}$, χ_1 is proper, $s \in \mathbb{Q}$, and in the formula (7.11) applied to χ_1 we have $a_v = 0$ for all v, then χ is called a *character of type* (A). If moreover, for totally positive $x \equiv 1 \bmod \mathfrak{f}$

one has

$$\chi(x) = \pm \prod_{v \in S_\infty} x_v^{r_v} \overline{x}_v^{s_v}$$

with $r_v, s_v \in \mathbb{Z}$, then χ is called a *character of type* (A_0). These characters were introduced by Weil [56], who showed that characters of type (A) have algebraic values, and the values of characters of type (A_0) associated with a field K lie in a fixed algebraic number field $L = L(K)$. The converse was established by Waldschmidt [81]. In Rohrlich [80c] zeta-functions of these characters were studied. There are deep relations between zeta-functions of such characters and certain zeta-functions of Abelian varieties, established by Taniyama [57].

These characters, and the corresponding zeta-functions were later studied in Iwasawa [75], Jensen [60], Kubert [85], Kubert, Lichtenbaum [83], C.G.Schmidt [80]. Lichtenbaum [82] presented a conjectural formula for $\zeta(0, J_a)$, and his conjecture has been proved by Brattström [82] for real Abelian fields, by Brattström, Lichtenbaum [84] for complex quadratic fields with odd class number, and by Anderson [86] for totally real fields and CM-fields. Anderson actually deduced Lichtenbaum's conjecture from a conjecture of Deligne [79], which in the considered cases is now a theorem. For totally real fields this follows from Siegel [80], and for CM-fields it has been done by Blasius [86]. For an exposition see Schappacher [88].

Weil [52a] showed that *Jacobi sums* (introduced by Jacobi [46] in certain special cases) are in fact Hecke characters. They are defined as follows: let $m \geq 2$, $K = \mathbb{Q}(\zeta_m)$, choose an unramified prime ideal $\mathfrak{p}$ in R_K and put $p = N(\mathfrak{p})$. Let χ_m be the m-th power character mod $\mathfrak{p}$, i.e.,

$$\chi_m(x)^m = 1 \quad \text{and} \quad \chi_m(x) \equiv x^{(p-1)/m} \pmod{\mathfrak{p}}.$$

For any $a = [a_1, \ldots, a_r]$ with $a_i \in \mathbb{Z}/m\mathbb{Z}$ put

$$J_a(\mathfrak{p}) = (-1)^{1+r} \sum \chi_m(x_1)^{a_1} \cdots \chi_m(x_r)^{a_r},$$

the summation extended over all $x_1, \ldots, x_r \bmod \mathfrak{p}$ satisfying $\sum x_1 \equiv -1 \bmod \mathfrak{p}$, and extend J_a by multiplicativity to all ideals of R_K, prime to mR_K. Weil showed that J_a is a Hecke character for all $a \neq [0, 0, \ldots, 0]$ (cf. Hasse [54b]). In Weil [74] this construction was extended to the case of arbitrary Abelian number fields. For conductors of these characters see R.F.Coleman, McCallum [88], Hasse [54b], Miki [94], Prapavessi [91]. Fields generated by $J_a(\mathfrak{p})$ were determined in Aoki [96].

If E is an elliptic curve with complex multiplication, then its L-function is expressible by zeta-functions of Hecke characters. This has been established by Deuring [53]. For an exposition see Gross [80]. There is a large literature concerning these functions, and the reader is advised to consult the book of Silverman [94].

Weil [52b] established an explicit formula for the limit

$$\lim_{T\to\infty} \sum_{|\mathrm{Im}\ \rho|<T} \Phi(\rho),$$

where

$$\Phi(s) = \int_{\infty}^{\infty} F(x) \exp((s-1/2)x)dx,$$

F is a complex-valued function satisfying suitable regularity conditions, and ρ runs over all zeros, satisfying $0 < \mathrm{Re}\ \rho < 1$, of a zeta-function associated with a Hecke character (see also Barner [81], Haran [90], Yagi [72]). The book of S.Lang [64] has a chapter devoted to this formula.

For the proof of Theorem 7.3 see Tate [50] and Tatuzawa [73b].

The *scalar product* of zeta-functions of Hecke characters χ_1 and χ_2 is defined by

$$Z(s, \chi_1, \chi_2) = \sum_{N(I)=N(J)} \frac{\chi_1(I)\chi_2(J)}{N(I)^s},$$

and a similar definition is used in the case of more characters. Vinogradov [65] continued this function to the half-plane $\mathrm{Re}\ s > 1/2$, and Kurokawa [78a,b], [86] obtained a necessary and sufficient conditions for the scalar product to be meromorphic in the case when all characters of finite order. The general case was treated in Moroz [82], who in [88] treated also scalar products of more general functions. For further results dealing with scalar products see the book of Moroz [86].

7. An important class of functions was introduced by Artin [24], [30b] and they are now called *Artin's L-functions*. Every such function is associated to a normal extension L/K and a character χ of a finite-dimensional representation of $Gal(L/K)$, and is denoted accordingly by $L(s, \chi, L/K)$, or simply by $L(s, \chi)$. If L/K is Abelian and χ is a character of an irreducible representation, then $L(s, \chi)$ coincides with the zeta-function of a suitable Hecke character of finite order.

Accounts of the theory of Artin's L-functions may be found in Hasse [26c], Heilbronn [67], Koch [90] and Martinet [77a]. Therefore we limit ourselves just to few remarks. It was shown by Brauer [47b] that every Artin's L-function is a product of powers (with rational integral exponents) of zeta-functions corresponding to Hecke characters of finite order in various fields, and thus, by Theorem 7.9, is meromorphic. Artin conjectured that they are entire, with some explicitly given exceptions. Class-field theory implies the validity of this conjecture for characters of one-dimensional representations, and Artin himself established it for monomial representations. In the two-dimensional case the occurring representations can be partitioned into four families — dihedral, tetrahedral, octahedral and icosahedral. Artin's conjecture in the dihedral case was established by Artin [24] himself, and for tetrahedral representations it was proved by Langlands [70] (for expositions of his proof see Gelbart [77], Gérardin, Labesse [79]), who also showed its truth for certain octahedral representations, and Tunnell [81] proved it in the octahedral case.

For certain classes of icosahedral representations the truth of Artin's conjecture was established in Buhler [78], Buzzard, Dickinson, Shepherd-Barron, Taylor [01], Kiming [94], Kiming, X.D.Wang [94], Ramakrishnan [91], Taylor [03]. In the general case Artin's conjecture would follow from Langlands conjectures concerning automorphic representations of GL_n. See Gelbart [84] on this topic.

For other results related to Artin's conjecture see Aramata [39], Foote [90], Foote, Wales [90], V.K.Murty [88], Sato [77], Uchida [75], Vinogradov [71], [73], van der Waall [73], H.Yoshida [77]. For a survey see Prasad, Yogananda [00].

Artin's conjecture is related to a question, considered in a special case already by Dedekind [00], and stated by Artin [23], whether the quotient $\zeta_L(s)/\zeta_K(s)$ is entire in case $K \subset L$. If L/K is normal then a positive answer gave Aramata [31], [33] and Brauer [47a]. See also Foote, Murty [89], Ishida [57], van der Waall [74b], [75], [82].

A similar conjecture has been posed by Brauer [73], who asked whether the ratio

$$\frac{\zeta_L(s)\zeta_k(s)}{\zeta_{K_1}(s)\zeta_{K_2}(s)}$$

is entire, where L is the composite of the fields K_1 and K_2, and k is their intersection. He showed that this is true if K_i/k are normal for $i = 1, 2$. In the general case only partial results are available (Sato [82], [83], [85], [86], van der Waall, Sato [93]).

The functional equation for Artin's L-functions contains a term $W(\chi)$ of absolute value 1. It is called the *Artin's root number*. Hasse [54a] posed the problem of factorization of $W(\chi)$ into local factors, and a solution was given, up to sign determination, by Dwork [56]. A complete solution has been announced in Langlands [70]. Another proof was given by Deligne [73] (cf. Deligne [76], Lakkis [66a], Tate [77]).

If the character χ is real-valued then $W(\chi) = \pm 1$, and it was shown in Fröhlich, Queyrut [73], that if χ is a character of a real representation, then $W(\chi) = 1$, but otherwise $W(\chi) = -1$ may occur. In Chap. 4 we noted the connection of the sign of $W(\chi)$ with the problem of the existence of normal integral bases.

For analogues of Gaussian sums associated with local factors of the root number see Fröhlich [83c], Fröhlich, Taylor [80], Martinet [77a]. Analogues of Jacobi sums have been considered in Bushnell [77a], Fröhlich [76b], [77c].

Stark considered in a series of papers (Stark [75a], [76a], [80]) the values of Artin's L-functions and their derivative at $s = 0$ and $s = 1$, and proposed certain conjectures. For Abelian extensions of totally real fields and of imaginary quadratic fields they are consequences of results of Siegel [70]. For expositions see Stark [82] and the book of Tate [84]. Proofs in special cases were obtained in Chinburg [83a], Sands [84a,b], [85], [87]. See also Bae [92], Chinburg [83c], Fröhlich [89], Stark [77a,b], Tate [81a,b].

For other results on Artin's L-functions see Barrucand [71], Goldfeld [73], Lagarias, Odlyzko [79], Odlyzko [77], Serre [71a], Suetuna [35], [36], [37], Weinstein [79], [80].

A still more general class of zeta-functions was introduced by Weil [51], who defined the *Artin-Hecke functions*, associated to characters of representations of a group $G_{L/K}$ defined for normal L/K as a certain extension of $C(L)$ by $Gal(L/K)$. They satisfy a functional equation, found by Tamagawa [53]. See Jehne [54], Lakkis [66b], [67], Tamagawa [51], Weil [71], [72].

6. An important class of functions, the *Selberg class* $\mathcal{S}$, encompassing many zeta-functions occurring in number theory, has been introduced by Selberg [92]. It consists of all functions $F(s)$ having the following properties:

(i) In the half-plane Re $s > 1$ F is the sum of an absolutely convergent Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$,

(ii) For every positive ϵ one has $a_n = O(n^{\epsilon})$,

(iii) For certain integer $m \geq 0$ the function $(s-1)^m F(s)$ is entire of finite order,

(iv) F satisfies a functional equation of the form

$$\Phi(s) = \omega \overline{\Phi}(1 - \bar{s}),$$

where $|\omega| = 1$, and

$$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s),$$

with some positive numbers Q, λ_j and μ_j lying in the half-plane Re $s \geq 0$,

(v) One has

$$\log F(s) = \sum_{n=1}^{\infty} b_n n^{-s},$$

where $b(n)$ vanishes, unless n is a prime power, in which case $b(n) = O(n^{\theta})$ with some $\theta < 1/2$.

The sum $2\sum_{j=1}^{r} \lambda_j$ is called the *degree* of F and is denoted by d_F.

Selberg proposed important conjectures concerning functions from the Selberg class:

(A) *If $F \in \mathcal{S}$, then with a positive integer n_F one has*

$$\sum_{p \leq x} \frac{|a_p|^2}{p} = n_F \log\log x + O(1),$$

and if F is primitive, i.e. cannot be written as a non-trivial product of two functions in $\mathcal{S}$, then $n_F = 1$.

(B) *If $F, G \in \mathcal{S}$ are both primitive, and $G(s) = \sum_{n=1}^{\infty} b_n n^{-s}$, then*

$$\sum_{p \le x} \frac{a_p \bar{b}_p}{p} = O(1).$$

(C) (The degree conjecture) *If $F \in \mathcal{S}$, then d_F is a non-negative integer.*

It follows from a result of Richert [57] (see also Conrey, Ghosh [93]) that the degree conjecture holds in the case $0 < d_F < 1$, and in Kaczorowski, Perelli [99a,V] this has been extended to the range $0 < d_F < 5/3$.

It turned out (Kaczorowski, Perelli [99a,I]) that if $F \in \mathcal{S}$ and $d_F = 1$, then F is a shift of a Dirichlet L-function associated with a primitive character (for another proof see Soundararajan [03]).

Conrey and Ghosh [93] proved that every non-constant function in $\mathcal{S}$ can be written as a product of primitive functions, and, moreover, the Selberg conjectures imply that this representation is unique.

These conjectures are very powerful, as they imply a part of Langland's conjectures, and also Artin's conjecture, which states that all non-trivial Artin L-functions are entire (M.R.Murty [94]).

For another conjecture, proposed by Sarnak see Kaczorowski, Perelli [99a,III], Vorhauer, Wirsing [01].

More about the Selberg class may be found in surveys of Kaczorowski, Perelli [99b] and M.R.Murty [94].

7. For the history of Corollary 2 to Proposition 7.12 see Narkiewicz [00].

Zeta-functions satisfy also certain approximate functional equations. For the Riemann zeta-function such an equation has been given by Hardy and Littlewood [23], but actually it goes back to Riemann (see Siegel [32]). For Dedekind zeta-functions of Abelian fields this was done by Gelfond [60], and for a large class of zeta-functions including all Dedekind's $\zeta_K(s)$ such equations were obtained in Chandrasekharan, Narasimhan [62b], [63] and Lavrik [68] (cf. Kaufman [78b]).

Theorem 7.15 for Dirichlet's L-functions is due to Dirichlet [38], and its general form is due to Hecke [18]. A proof based on class-field theory may be found in the book of Weil [67] (Chap. XIII, Th.11).

The *Great Riemann Hypothesis* (*GRH*) asserts that no zeta-function of a proper Heche character has a zero in the open half-plane Re $s > 1/2$. It is also conjectured that all zeros on Re $s = 1/2$ are simple. The largest zero-free region for $\zeta_K(s)$ was obtained by Mitsui [68] and Sokolovskiĭ [68]. They proved that $\zeta_K(\sigma + it) \neq 0$ in the region

$$\sigma \ge 1 - C \log^{-2/3} t (\log\log t)^{-1/3}, \quad |t| \ge t_0$$

with suitable positive constants C and t_0 depending on K (for earlier results see Landau [19b], [24a]). It was shown by Bartz [78] that one can take $t_0 = 4$ and $C = cn^{-11}|d(K)|^{-3}$, with $n = [K : \mathbb{Q}]$ and c independent of K. See also Werbiński [88].

A similar zero-free region has been established by Hinz [80] for zeta-functions of every Hecke characters χ of finite order. In this case the involved constants depend additionally on the conductor of χ (see also Bartz [85]). The case of characters of infinite order has been considered by M.D.Coleman [90].

The first bound for values of the Dedekind zeta-function appeared in Landau [03a]: $\zeta_K(1+it) = O(\log|t|)$. Sokolovskiĭ [68] improved this bound to $O(\log^{2/3}|t|)$. Lower bounds for $\zeta(1,\chi)$, where χ is a character of the class-group, gave Landau [19a]. For other bounds for $\zeta_K(s)$ and certain other zeta-functions in the strip $0 < \mathrm{Re}\ s \leq 1$ see Bartz [88], Bartz, Staś [86], Heath-Brown [88], Hinz [79], Kaufman [78a,b], [79], Motohashi [70], Staś [76], [79], Weinstein [77], Wieczorkiewicz [79].

Asymptotics for $\int_0^T |\zeta_K(1/2+it)|^2 dt$ was found in Müller [89a].

Large values of $|\zeta_K(s)|$ for quadratic K were considered in Balakrishnan [86], who generalized a result of Montgomery [77], dealing with Riemann's $\zeta(s)$.

Mean values of the functions $\zeta(s,\chi)$, where χ are characters of $H(K)$ for imaginary quadratic fields K were studied in Duke, Friedlander, Iwaniec [95].

8. Denote by $N_K(\sigma,T)$ the number of zeros ρ of $\zeta_K(s)$ satisfying $\mathrm{Re}\ \rho \geq \sigma$ and $|\mathrm{Im}\ \rho| \leq T$, each counted according to its multiplicity. From *GRH* the equality $N_K(\sigma,T) = 0$ follows for $\sigma > 1/2$, and so it is of interest to obtain unconditional upper bounds for $N_K(\sigma,T)$. The best result here is due to Heath-Brown [77], who for every $\epsilon > 0$ got

$$N_K(\sigma,T) \ll T^{(n+\epsilon)(1-\sigma)} \log^C T,$$

with $C = C(\epsilon,K)$ and $n = [K:\mathbb{Q}] \geq 3$, uniformly for $1/2 \leq \sigma \leq 1$, and obtained a similar result in case $n = 2$. The *Density Hypothesis*, which is weaker than *GRH*, claims that

$$N_K(\sigma,T) \ll T^{2(1-\sigma)+\epsilon} \log^C T$$

holds uniformly for $1/2 \leq \sigma \leq 1$ with $C = C(\epsilon,K)$. In the case $K = \mathbb{Q}$ the Density Hypothesis for $\sigma \geq 11/14$ was established by Jutila [77], who also proved it for $\sigma \geq 21/26$ for Abelian fields. Cf. Heath-Brown [77], Sokolovskiĭ [66], Wieczorkiewicz [80].

Similar questions for various classes of zeta-functions have been studied in Bartz, Fryska [89], Bulota [63], [64], Duke [89], Fogels [65], [71], [72], Hilano [74], Hinz [76], Johnson [79], Maknis [75a,b], [76].

A lower bound ($\gg T^{6/11}$) for the number of simple zeros ρ in the rectangle $0 < \sigma < 1$, $0 < t < T$ of $\zeta_K(s)$ for quadratic K was proved in Conrey, Ghosh, Gonek [86], and a much better bound ($\gg T\log T$) is a consequence of the Riemann Hypothesis.

Heilbronn [72], [73] proved that if L/K is normal, then every real simple zero of $\zeta_K(s)$ is already a zero of a Dedekind zeta-function of a quadratic extension of K contained in L. It is an old unsolved question whether Dedekind zeta-functions of quadratic fields may have zeros in the interval $(0,1)$. This question is related to the magnitude of the class-number (see Chap. 8). It has been proved in Conrey, Soundararajan [02] that for at least 20% of negative even quadratic discriminants the function $\zeta_K(s)$ does not have real zeros. Moreover, this is true (Watkins [04a]) for all imaginary quadratic fields K with $d(K) \leq 3 \cdot 10^8$. Cf. Çallial [80], P.Chowla [74], S.Chowla [36], Chowla, Erdős [51], Chowla, Hartung [74b], Chowla, de Leon [74], Chowla, de Leon, Hartung [73], Heilbronn [37], Louboutin [03], Low [68], Purdy [72], Rosser [49].

For fields of higher degrees the equality $\zeta_K(1/2) = 0$ may well happen, as the example $K = \mathbb{Q}(a,b,c)$ with $a = \sqrt{5}$, $b = \sqrt{41}$, $c = \sqrt{(5+a)(41+ab)}$ shows, found by Armitage [72]. The fact that zeta-functions of a large class of Hecke characters do not vanish at $s = 1/2$ has been established in Montgomery, Rohrlich [82] and Rohrlich [80a,b].

Landau [19b] showed that there exists $C = C(n)$ such that for any real T all Hecke zeta-functions of a field of degree n have a zero in the rectangle $1/2 \leq \operatorname{Re} s < 1$, $T \leq \operatorname{Im} s \leq T + C$, and later Siegel [72a] proved that C may be taken independent of n. Let $z(K)$ be the minimal imaginary part of a zero of $\zeta_K(s)$. It was proved by Neugebauer [88] that for fixed $[K : \mathbb{Q}]$ one has $z(K) \ll 1/\log\log\log|d(K)|$. In Tollis [97] it has been conjectured that $z(K) \leq C/\log|d(K)|$, where C depends only on the degree of K, and Omar [00] showed that *GRH* leads to the bound $z(K) \ll 1/\log\log|d(K)|$, with the implied constant depending on the degree of K. Evaluations of $z(K)$ for totally complex fields with small degrees and discriminants were given in Omar [01].

In Chowla, Goldfeld [76] several Hecke zeta-functions without zeros in the interval $(0,1)$ were found.

For other results dealing with zeros of zeta-functions see Fogels [63], Fryska [79], [91], Fujii [77], Greenberg [85], [87], Haselgrove [51], Hinz [77], Hinz, Lodemann [94], Odlyzko, Skinner [93], Rohrlich [92].

9. The *partial zeta-function* of a class X of $H_I(K)$ or $H_I^*(K)$ is defined for $\operatorname{Re} s > 1$ by

$$Z(s,X) = \sum_{I \in X} \frac{1}{N(I)^s}.$$

Theorem 7.9 implies that $Z(s,X)$ can be prolonged to a meromorphic function (this is a result of Hecke [17a]). From a result of Potter and Titchmarsh [35] it follows that for imaginary quadratic K the function $Z(s,X)$ has infinitely many zeros on the line $\operatorname{Re} s = 1/2$ (cf. Hecke [37]), and the same holds also for real quadratic fields (Chandrasekharan, Narasimhan [68], cf. Berndt [71a]). For certain other classes of fields see Berndt [70], Czarnowski

[82]. Zeros of partial zeta-functions of quadratic fields lying on the critical line were considered in Sankaranarayana [95]. A link between the existence of an ideal of small norm in X, and real zeros, close to 1, of $Z(s, X)$ was established in Friedman [87].

Let K be an imaginary quadratic field and let X be a class in $H(K)$. An explicit value for

$$a_0(X) = \lim_{s \to 1} ((s-1)Z(s, X) - \kappa)$$

was given by Kronecker [85] (*Kronecker's limit formula*). See Siegel [61] for a proof and various applications (cf. Ramachandra [64], [69], Shintani [80a], Zagier [75a]). For an analogous result in real quadratic fields see Hecke [17d], Herglotz [23], Novikov [80], Shintani [77a], . Certain quartic fields were treated in Hara [93], Katayama [66] and Konno [88], and the case of CM-fields was settled in Konno [65]. Finally, an analogue of Kronecker's formula for all algebraic number fields was obtained by Goldstein [74]. For values of $Z(s, X)$ at $s = 0$ in the case of real quadratic fields see Hayes [90].

Partial zeta-functions in totally real fields were treated by Shintani [76a], who expressed them as finite sums of simpler Dirichlet series, and in Shintani [80b] the same result was obtained for arbitrary fields.

10. Much attention has been attracted by the values of various zeta-functions at particular points, mostly at integers and rationals. It seems that many properties of algebraic number fields are encoded in those values. As an example of this philosophy one can take the junction between the vanishing of $\zeta_K(s)$ at $s = 1/2$, and the existence of a normal integral basis in the case when $K/\mathbb{Q}$ is tame, and has the quaternion Galois group; we discussed this in Chap. 4. A very general conjecture relating the values of various zeta-functions at integers to integrals of differential forms on varieties appears in Deligne [79].

The values of $\zeta(s)$ at even positive integers have been computed already by Euler, and the analogous question for Dedekind's zeta-function of $\mathbb{Q}(i)$ has been dealt with by Hurwitz [99]. Later Hecke [21a,II] considered real quadratic K, and asserted that for even $s > 0$ and every class $X \in H^*(K)$ the equality

$$Z(s, X) = r(s, X)\pi^{2s}\sqrt{d(K)}$$

holds with a certain non-zero rational $r(s, X)$. This clearly would imply a similar assertion for $\zeta_K(s)$, and it would follow from the functional equation that for $k = 1, 2, \ldots$ the value $\zeta_K(1 - 2k)$ is rational. Hecke's assertion was established in H.Lang [68], Meyer [67], Siegel [69b] (cf. Siegel [37]). Analogues for $Z(s, X)$ with $X \in H_I^*(K)$ have been obtained in the case of totally real K by Klingen [62] and Siegel [70].

Serre [71b] posed two conjectures concerning the value of $\zeta_K(s)$ for totally real K at negative odd integers. The first asserts that if p is a rational prime and $\mathfrak{p}$ is a prime ideal lying over p in R_K, then the denominator of

$$\frac{N(\mathfrak{p})^{2k}-1}{2^n}\zeta_K(1-2k)$$

(where $n=[K:\mathbb{Q}]$), is a power of p for $k=1,2,\ldots$, and the second states that the ratio $\zeta_K(1-2k)/\zeta(1-2k)$ is a rational integer, divisible by an explicitly given power of 2. For Abelian K these conjectures were proved in Fresnel [71] and Coates, Lichtenbaum [73]. The first of Serre's conjectures can be deduced from more general conjectures of Lichtenbaum [72] and Coates, Lichtenbaum [73], which express, in particular, the exponent of a prime occurring in the factorization of $\zeta_K(1-2k)$ (and, more generally, of $L(1-2k,\chi,L/K)$) in terms of p-adic cohomologies. These conjectures were in turn deduced by Bayer, Neukirch [79] from the "Main Conjecture" (see Coates [77], and the second edition of S.Lang [78]), which is now a theorem, due to the work of Mazur, Wiles [84] (see Coates [81] and S.Lang [82] for expositions), and so is Serre's first conjecture.

The value $\zeta_K(-1)$ is related to the theory of quaternion algebras (see Guého [72a,b], [74a,b], Vignéras [74], [75a,b]). A formula for this value in terms of subgroups of $SL_2(R_K)$ was obtained in K.S.Brown [74] and Hirzebruch [73]. Values of Artin L-functions at integers were studied in Taylor [81c].

For other results dealing with values of $\zeta_K(s)$, $Z(s,X)$, and other zeta-functions at integers and rationals see Barner [68], [69], Borel [77], P.Cassou-Noguès [79], Coates, Sinnott [77], H.Cohen [74], [76], Eie [89], Gundlach [73], Halbritter, Pohst [90], Hida [78], Kallies, Snyder [95], Katayama [76], Kramer [87], H.Lang [68], [72], [73a,b], [85b], Meyer [67], Okazaki [91], Shintani [76b], [77b], [81], Siegel [68a], [75], Toyoizumi [81a,b], [82], Zagier [76], [77], [86], [91].

11. Proposition 7.16 is due to Landau [18f], as well as most corollaries to it. Corollary 5 got an elementary proof in Babaev [71]. A version of Corollary 6 occurs in Furtwängler [07], and its general form, for classes of $H_I(K)$, in Hecke [17c], who also established Corollary 7 in that case. Corollary 7 was proved by Dirichlet [41b] for $K=\mathbb{Q}(i)$, and by Fanta [01] for $K=\mathbb{Q}(\zeta_3)$.

Bounds for the least non-splitting prime in a given field were found in V.K.Murty [94], Vaaler, Voloch [00]. For real quadratic fields see Granville, Mollin, Williams [00].

For evaluation of character sums occurring in Proposition 7.17 (i) see Barban, Levin [68], Fogels [65], Friedlander [73], [74], Hinz [83a,b], Jordan [67], Lee [79].

12. Corollary 1 to Proposition 7.17 (usually called the *Prime Ideal Theorem*) was conjectured in Landau [03a], and proved in Landau [03b]. Previously only upper and lower bounds for $\pi_K(x)$ were known, similar to those obtained by Chebyshev in the case $K=\mathbb{Q}$ (see Landau [03a], Phragmén [92], Poincaré [92], Torelli [01]).

Other proofs of the Prime Ideal Theorem were given in Ahern [64] and Rieger [59], both covering also Corollary 4 to Proposition 7.17. The first elementary proof was given by Shapiro [49], who utilized an analogue of Selberg's lemma. For Selberg's lemma in this context see Ahern [65], Ayoub [55], G.L.Cohen [75b], Rieger [58a,b], [61c], K.Yamamoto [58]. Other elementary proofs appeared in Bredikhin [58], Eda, Nakagoshi [67], Forman, Shapiro [54], Hinz [93]. A proof based on the large sieve method gave Touibi, Zargouni [89].

Landau's proof gave in the Prime Ideal Theorem the bound

$$O(x \exp(-\log^{1/13} x)).$$

The remainder given by us in Corollary to Theorem 7.20 is due to Landau [18f]. The best evaluation at this moment, namely

$$O\left(\exp(-C \log^{3/5} x (\log\log x)^{-1/5})\right),$$

with a certain $C > 0$, is due to Mitsui [68] and Sokolovskiĭ [68]. The dependence of that bound on K was investigated in Goldstein [70a] and Wiertelak [78]. See Friedlander [80], Révesz [83], Sokolovskiĭ [71] for other results concerning $\pi_K(x)$. Sign changes of the error term in the Prime Ideal Theorem in the form

$$\sum_{N(\mathfrak{p}^m) \leq x} \log N(\mathfrak{p}) = x + R(x)$$

were studied in Kaczorowski, Staś [88] and Szydło [89].

Theorem 7.20 shows that an enlargement of the zero-free region of zeta-functions leads to an improved bound for the remainder term in the asymptotic formula for the corresponding counting function. This dependence can be reversed. In the case of the rational field this has been shown by Turán [50], [53; sect.9,13], and for arbitrary K this result is due to Staś [59], [60], [61], and Staś, Wiertelak [75], [76a].

Corollary 4 to Proposition 7.17 for classes of $H(K)$ was proved by Landau [07]. His proof was based on a result of Furtwängler [07] giving the existence of the Hilbert class-field of K, since at that time the continuation of the zeta-functions beyond Re $s = 1$ was not known. For classes of $H_I(K)$ and $H_I^*(K)$ this result is due to Hecke [17c] and Landau [18f], respectively. A uniform evaluation of the remainder term, valid for $N(I) \ll \exp(c \log\log x / \log x)$, was obtained by Hinz [76], [80] (cf. Staś, Wiertelak [76b]). This result generalizes Dirichlet's theorem on primes in progressions and is often called *Hecke's theorem on progressions*. For early results for $K = \mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$ see Fanta [01], H.Weber [05].

The analogue of Linnik's theorem on primes in progressions was established by Fogels [61], [62a,b], [65], [66a] and Rieger [61a] in the following form:

In every class of $H_I^*(K)$ there exists a prime ideal of norm not exceeding $cN(I)^b$, with certain constants b, c, depending on K.

See also Lagarias, Odlyzko [77], A.Weiss [83].

An analogue of the Brun-Titchmarsh theorem for $\pi_X(x)$ was proved in Hinz, Lodemann [94]. The Barban-Davenport-Halberstam theorem for progressions has been generalized to algebraic number fields in Hinz [81], [96].

For various generalizations of Bombieri's prime number theorem to algebraic number fields see Hinz [88], [96], Huxley [68,III], Murty, Murty [87], R.J.Wilson [69]. The large sieve in these fields was considered in Huxley [68], Maknis [80], Schaal [70], and Schumer [86], and Linnik's sieve in Rieger [60], [61b]. For Selberg's sieve and its applications see Hinz [82], [03], Rieger [58e], Sarges [76], Schaal [68], Vinogradov [64]. For a generalization of the Rosser-Iwaniec sieve see M.D.Coleman [93]. For a survey of sieve methods in algebraic number fields see Schaal [84].

13. The *Ideal Theorem* (Corollary to Theorem 7.18) is due to Dedekind [71], and Theorem 7.18, in its most general form, to Landau [18f]. This paper of Landau, which we quoted already several times, contains a detailed treatment of zeta-functions associated with characters of $H_I^*(K)$. For the Ideal Theorem see also H.Weber [96a] and Wintner [45].

Landau [18e,f] showed that the error term in Theorem 7.18 (hence also in the Ideal Theorem) is $O\left(x^{1-c}\right)$ with $c = 2/(1+n)$ for fields of degree n. The dependence of the constants on K was in case $I = R_K$ made explicit in Fogels [66a]. Tatuzawa [73a] improved the error term, and made the involved constant explicit. At this moment the best evaluation of the error term in the Ideal Theorem is due to Nowak [93], who showed that it is $\ll x^{1-\alpha_n} \log^{\beta_n} x$ with

$$\alpha_n = \begin{cases} \frac{2}{n} - \frac{8}{5n^2+2n} & \text{if } 3 \le n \le 6, \\ \frac{2}{n} - \frac{3}{n^2} & \text{if } n \ge 7, \end{cases}$$

and

$$\beta_n = \begin{cases} \frac{10}{5n+2} & \text{if } 3 \le n \le 6, \\ \frac{2}{n} & \text{if } n \ge 7. \end{cases}$$

For quadratic fields the best known evaluation is $O(x^a \log^b x)$ with $a = 23/73$ and $b = 315/436$, obtained by Huxley [00] (cf. Ayoub [68], Huxley, Watt [94], Müller [89b], Arnold Walfisz [26])), and for cubic fields it is $O(x^a)$ with any $a > 43/96$ (Müller [88]). For cyclotomic fields see Karatsuba [72].

One sees immediately that if for $m = 2, 3, \ldots$ we write

$$\zeta_K(s)^m = \sum_I \frac{d_m(I)}{N(I)^s},$$

then $d_m(I)$ would be the number of representations of I as a product of m ideals. In particular $d_2(I)$ is the number of divisors of I. It follows from a general result of Landau [12a] that with a polynomial P_{m-1} of degree $m-1$ one has

$$\sum_{N(I) \le x} d_m(I) = x P_{m-1}(\log x) + O(x^\alpha),$$

with any $\alpha > 1 - 2/(mn+1)$, n being the degree of K. This bound cannot be replaced by $\alpha > (mn-1)/2mn$ (Landau [24b]), and later it was shown that even $a = (mn-1)/2mn$ is impossible (Chandrasekharan, Narasimhan [62a], Joris [72]). The problem of evaluating the error term is called the *Piltz divisor problem.*

For other results dealing with the coefficients of $\zeta_K(s)$, or its powers, and the analogues of classical divisor problems see R.G.Ayoub [58], Berndt [69], [71b], [75], Chandrasekharan, Good [83], Chandrasekharan, Narasimhan [62a,b], [64], van der Corput [23], Dzhiemuratov [68], Eda [55], Grotz [80], Hafner [83], Hasse, Suetuna [31], Iseki [53], Kanemitsu [78], Lai [65], Landau [03a], [12b], [25], Linnik, Vinogradov [66], Odoni [91b], Rausch [90], [94], Rieger [57], [58c], Suetuna [25a,b], [28], [29], [31], Szegő, Walfisz [27], Tatuzawa [77], Anna Walfisz [64], Arnold Walfisz [25], [26], Warlimont [67].

Proposition 7.19 is due to Wirsing (see Ostmann [68,II,p.67). For the field $\mathbb{Q}(i)$ it goes back to Landau [08] (see also Luthar [66]). Its extension to non-normal extension appears in Odoni [75a]. Asymptotic behaviour of the number of positive rational integers $\leq x$ which are norms of fractional ideals of K, and norms of principal fractional ideals of K, respectively, has been determined in Odoni [73b]. See also Odoni [75b], [77a,b], [78], [89], L.P.Schmid, Shanks [66], Wintner [46a].

14. Hecke [18] used his zeta-functions to prove uniform distribution in sectors of points $(x,y) \in \mathbb{R}^2$ such that for a fixed quadratic form the value $f(x,y)$ is a rational prime. In case of the field $Q(i)$ this is related to the representation of primes $p \equiv 1 \pmod 4$ as sums of two squares. Hecke's result implies a.o. that there are infinitely many primes of the form $p = a^2 + b^2$ with $b = o(\sqrt{p})$. Assuming *GRH* one can replace in this equality the term $o(p)$ by $o(\log p)$ (Ankeny [52b]). Unconditionally it is known that $b = O(p^c)$ is possible with $c = 0.1631$ (M.D.Coleman [93]). This has been put in a more general setting in S.Lang [64] and Mautner [53]. Another proof of Hecke's theorem in the case of imaginary quadratic fields gave Knapowski [69]. Evaluations of the remainder term were provided in Kubilius [52], and Mitsui [56] made them uniform. See also Bulota [64], Kaufman [77], Korchagina [79], Kovalchik [74], [75], Maknis [75a,b], [76], [80], Rademacher [35], [36a,b], Schulz-Arenstorff [57], Urbelis [64], [65a,b], Zarzycki [91].

The problem of counting Gaussian primes in sufficiently regular subsets of the plane was considered by Chulanovskii [56], and his results were extended by G.L.Cohen [75a,b]. Cf. Hensley [76]. It has been established by M.D.Coleman [98] that if $\Phi(t)$ tends to infinity with t, then for almost all complex z_0 the disc

$$\{z : \ |z - z_0| < \Phi(|z|) \log |z|\}$$

contains at least one Gaussian prime. The distribution of Gaussian integers of a given norm N on the circle $|z| = \sqrt{n}$ was studied in Erdős, Hall [99]. For almost all n this distribution is approximately uniform.

15. The symbol $F_{L/K}$ was introduced by Artin [24], and is usually called the *Artin symbol*. The first step toward Theorem 7.30 was done by Frobenius [96], who proved Proposition 7.35 (i). Other proofs appear in Chebotarev [26], Hasse [26c,II, sect.24], Hurwitz [26], Schreier [27]. Part (ii) of this proposition is essentially due to Kronecker [80], who tacitly assumed the existence of the densities d_i.

The first proof of Theorem 7.30 was given by Chebotarev [23b], [26] (see also [37c]). His proof was simplified in Deuring [35a], MacCluer [68], Scholz [31] and Schreier [27]. Purely algebraic proofs in certain special cases were given in Lenstra, Stevenhagen [91] and Wójcik [75]. Proofs leading to explicit evaluation of the error term in Theorem 7.30, and also of the smallest norm of a prime ideal in a conjugacy class have been obtained in Lagarias, Montgomery, Odlyzko [79], Lagarias, Odlyzko [77], Schulze [72,III].

For a generalization of Theorem 7.30 see Odoni [77a], and for a conjecture related to it see Lenstra [77b]. The analogue of it for infinite extensions is false. This follows from an old result of Moriya [34a], but Serre [81] proved such a generalization in certain special cases. The paper of Serre contains also applications of Theorem 7.30 to the theory of elliptic curves and modular forms.

For other questions around Theorem 7.30 see Jarden [74].

16. Proposition 7.36 is due to Artin [23], and Lemma 7.39 to Hasse [30a]. Lemma 7.37 in a more precise form, taking into account also ramified primes, occurs in van der Waerden [34]. Cf. Bauer [37], Wegner [35]. The notion of a Bauerian field and Theorem 7.38 are due to Schinzel [66]. Corollary 1 to that theorem was proved by Bauer [16a]. For another proof see Deuring [35b], and for applications see Ankeny, Rogers [51], Flanders [53b], Mann [54], [55].

The first example of a non-Bauerian extension was given by Gassmann [26]. For other examples see Gerst [70], Lewis, Schinzel, Zassenhaus [66], and Schinzel [66]. In the last paper it is also shown that all fields of degree ≤ 4 are Bauerian. For similar questions see Bilhan [81], Nakatsuchi [68], [70], [72], [73], [75].

It follows from Theorem 4.33 that if $f \in \mathbb{Z}[X]$ is the minimal polynomial of an integral generator of $K/\mathbb{Q}$, then $P(K/\mathbb{Q})$ differs from $P(f)$, the set of all primes p for which the congruence $f(x) \equiv 0 \pmod{p}$ is solvable, only by finitely many elements. A survey of the properties of $P(f)$ was given by Gerst, Brillhart [71]. See also Nagell [68a], Schinzel [68], Schulze [72], [73], [76a,b].

Two extensions L_1/K and L_2/K are called *Kronecker equivalent*, if the sets $P(L_1/K)$ and $P(L_2/K)$ differ only by finitely many elements. (Note that arithmetic equivalence of fields implies their Kronecker equivalence.) The resulting equivalence classes are called *Kronecker classes*. This notion is due to Jehne [77b], who showed that all minimal elements of a Kronecker class have the same Galois hull over K (i.e., the smallest normal extension of K, containing such field). He gave also examples of infinite Kronecker classes.

Towers of fields with the same Kronecker class were studied in Klingen [78] (cf. Komatsu [82]). For other problems on Kronecker classes see Jehne [77c], Klingen [79], [80], [83], Lochter [93], [94a,b], [95], Saxl [88], Schulze [81]. See also the book of Klingen [98].

Theorem 7.40 is due to Hilbert [97], and the proof given by us is that of Chebotarev [23a] (cf. Chebotarev [37c], Rabung [70], Wójcik [69]). For generalizations see Elliott [70a], Mills [63], Shafarevich [54].

A generalization of Lemma 7.41 (i) to composite p was for $K = \mathbb{Q}$ obtained by Gerst [70], and for arbitrary fields of characteristic not dividing p by Schinzel [75b]. They noted that the generalization given in Nagell [39] is inexact, as the example $K = \mathbb{Q}$, $p = 8$, $a = -1$, $b = 16$ shows. For generalizations of Lemma 7.41 (ii) see Besicovitch [40], Halter-Koch [80], M.Kneser [75], Mordell [53], Schinzel [75b], Siegel [72b], Ursell [74]. Cf. also Mostowski [55], Roth [71].

A conjecture concerning the density of the set of all primes which do not split in fields from a certain infinite family closed under composition was stated by Goldstein [68], [70b]. Although it turned out to fail in general (Weinberger [72c]), it holds nevertheless in certain interesting cases (Goldstein [71a], [73a], M.R.Murty [83], [84]).

17. Theorem 7.42 is due to Fröhlich [60a,b,d], and our exposition is based on his work. Corollary 3 to it fails to hold in the case of even class-number, as shown by Pierce [74]. The R_K-module structure of ideals in an extension L/K was dealt with in Fröhlich [60c].

The first necessary and sufficient condition for the existence of a relative integral basis (RIB) was given by Artin [50a]: if $L = K(a)$ with $a \in R_L$ then the fractional ideal $d_{L/K}^{-1}(a)d(L/K)$ is a square of a fractional ideal I, and RIB exists if and only if I is principal (cf. Fujisaki [74], Hecke [12]). For simple examples of extensions without RIB see Edgar [79], MacKenzie, Scheunemann [71].

Corollary to Proposition 7.46 is due to Mann [58].

Conditions for the existence of RIB in particular classes of extensions have been considered in Bird, Parry [76], Edgar, Peterson [80], Feng, Zhang X. [83], Hymo, Parry [90], [92], Martinet, Payan [67], [68], McCulloh [63], [71], Schmal [89], Sergeev [73], Soverchia [02], Spearman, Williams [88], [96b], Wada [70], Washington [76a], Zhang X. [84d,e].

Proposition 7.47 shows that Steinitz classes of normal extensions of a given degree need not cover $H(K)$. Denote by $R(K,G)$ the set of Steinitz classes of normal extensions of K with Galois group G. For cyclic p-groups this set was determined in Long [71], [75] (cf. Long [72]). Steinitz classes for other extensions were considered in Carter [96], [97], [98], [99], Godin, Sodaïgui [02], [03], Hutchinson [95b], Massy, Sodaïgui [97], Sodaïgui [97], [99] [00a,b].

18. Let Ω_p be the completion of the algebraic closure of $\mathbb{Q}_p$. Kubota and Leopoldt [64] defined p-adic analogues $L_p(s,\chi)$ of Dirichlet's L-functions, associated with non-principal Dirichlet characters as the unique continuous function defined on a neighbourhood of zero, which for all positive integers n, divisible by $p-1$, if p is odd, and even, if $p=2$, satisfies

$$L_p(1-n,\chi) = (1-\chi(p)p^{n-1}L(1-n,\chi).$$

Accounts on the theory of these functions are given in Colmez [00], Iwasawa [72a], Koblitz [77], and Washington [82].

The "Main Conjecture" of Iwasawa, proved in Mazur, Wiles [84], asserts, roughly speaking, that if p is an odd prime, and ω_p is the *Teichmüller character* of $\mathbb{Z}_p$ (defined for $x \in \mathbb{Z}_p$ as the unique root of unity of order $p-1$ such that for all $x \in \mathbb{Z}_p$ one has $x \equiv \omega(x) \pmod{p}$), then the zeros of $L_p(\omega_p^j, s)$ are related to p-components of the class groups of cyclotomic fields of p-power order.

Local versions of L-functions over arbitrary totally real fields were defined in Barsky [77], P.Cassou-Noguès [79], and Deligne, Ribet [80].

In a similar fashion Serre [73] defined the p-adic analogue of Dedekind zeta functions for totally real extensions of $\mathbb{Q}$. The residue of this function at $s=1$ was determined in Colmez [88]. For the Abelian case see Amice, Fresnel [72], Fresnel [67], Leopoldt [75].

EXERCISES

1. Compute $\zeta_K(0)$ for imaginary quadratic K.

2. Let K be an algebraic number field and denote by $\mathcal{F}(\mathcal{K})$ the set of all complex-valued functions f, g defined on the set of all non-zero ideals of R_K. For any two functions f, g of $\mathcal{F}(\mathcal{K})$ define their *Dirichlet convolution* by

$$(f*g)(I) = \sum_{J|I} f(J)g(IJ^{-1}).$$

(i) Prove that the set $\mathcal{F}(\mathcal{K})$ forms a commutative ring with unit under usual addition, and Dirichlet convolution as multiplication.

(ii) Prove that $f \in \mathcal{F}(\mathcal{K})$ has an inverse if and only if $f(R_K) \neq 0$.

(iii) A non-zero function $f \in \mathcal{F}(\mathcal{K})$ is called *multiplicative* if for $(I,J)=1$ one has $f(IJ) = f(I)f(J)$. Prove that if f, g are multiplicative so is $f*g$.

(iv) Prove that the inverse of a multiplicative function is multiplicative.

2. Let $h = f*g$ and assume that the series

$$\mathfrak{F}(s) = \sum_I F(I)N(I)^{-s}, \quad \mathfrak{G}(s) = \sum_I G(I)N(I)^{-s}$$

are absolutely convergent in a certain half-plane. Prove that the series

$$\mathfrak{H}(s) = \sum_I H(I)N(I)^{-s}$$

converges absolutely in that half-plane and one has $\mathfrak{H}(s) = \mathfrak{F}(s)\mathfrak{G}(s)$.

3. Let $d_m(I)$ be the number of representations of the ideal I as a product of m factors (representations differing by the order of the factors being regarded as distinct). Prove that for Re $s > 1$ the series

$$\sum_I d_m(I) N(I)^{-s}$$

converges absolutely, and its sum equals $\zeta_K^m(s)$.

4. Let X be a class in $H_{\mathfrak{f}}^*(K)$.

(i) Prove that for x tending to infinity one has

$$\sum_{\substack{I \in X \\ N(I) \leq x}} d_m(I) = (c + o(1)) x \log^{m-1} x,$$

with

$$c = \frac{1}{(m-1)!} \frac{h(K)^m \kappa^m \varphi(\mathfrak{f})^m}{h_{\mathfrak{f}}^*(K) N(\mathfrak{f})^m}.$$

(ii) Prove that

$$\sum_{\substack{\mathfrak{p} \in X \\ N(\mathfrak{p}) \leq x}} \frac{1}{N(\mathfrak{p})} = \frac{1}{h_{\mathfrak{f}}^*(K)} \log \log x + B + O\left(\frac{1}{x}\right)$$

with a certain $B = B(K)$.

5. Determine explicitly all Hecke characters of the fields $\mathbb{Q}$ and $\mathbb{Q}(i)$.

6. Show that if χ is a quasicharacter of I_K trivial on I_0, and Ω is the group consisting of all ideles $\xi = \langle x_v \rangle$ with $x_v = 1$ for non-Archimedean v's, then the equality

$$\chi(\xi) = \prod_{v \in S_\infty} \left(\frac{x_v}{|x_v|}\right)^{n_v} v(x_v)^{s + i a_v}$$

holds on Ω with suitable rational integers n_v, real a_v and a complex s.

7. (Weil [56]) (i) Prove that every Hecke character of type (A) has algebraic values.

(ii) Prove that all values of a Hecke character of type (A_0) lie in a finite extension of $\mathbb{Q}$.

(iii) Let χ be a character of $H_I^*(K)$ for a certain ideal I, and let $r \in \mathbb{Q}$. Show that $X(I) = \chi(I) N(I)^r$ is a Hecke character of type (A).

(iv) Let K be a CM-field. Prove the existence of Hecke characters of type (A) which are not of the form given in (iii).

(v) Prove that all Hecke characters of type (A) of a field K have the form given in (iii) if and only if K does not contain any CM-field.

8. Prove that all prime ideals lying in $P(L/K)$ split if and only if L/K is normal.

9. (Hecke [17c]) Prove that for every ideal I and $a \in R_K$, satisfying $(aR_K, I) = 1$ there exist infinitely many non-associated elements c congruent to a mod I, and generating prime ideals of first degree.

10. (Bilhan [81]) Let $P_0(L/K)$ be the set of all prime ideals of R_K which split in L/K. Prove that if $P(L/K) \subset P_0(M/K)$ then $M \subset L$.

11. Prove that the set of all prime ideals of K which have at least one prime ideal factor of degree one in L/K has Dirichlet density $\geq 1/[L : K]$, equality holding if and only if the extension L/K is normal.

12. Prove that if $h(K) = 3$, then every cyclic extension of K of degree seven has a relative integral basis.

8. Abelian Fields

8.1. Main Properties

1. This chapter is devoted to the arithmetic of Abelian extensions of the rationals, i.e., normal extensions $K/\mathbb{Q}$ with an Abelian Galois group. According to the Kronecker-Weber theorem (Theorem 6.18) every such extension is contained in a suitable cyclotomic field $K_n = \mathbb{Q}(\zeta_n)$. The least integer f with the property $K \subset K_f$ is called the *conductor* of K, and is denoted by $f(K)$. The main properties of the conductor are listed in the following proposition:

Proposition 8.1. *Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be Abelian.*

(i) $K \subset K_m$ holds if and only if $f(K)$ divides m.

(ii) $f(K \cap L)$ divides $(f(K), f(L))$,

(iii) $f(KL) = [f(K), f(L)]$,

(iv) A prime p ramifies in $K/\mathbb{Q}$ if and only if $p|f(K)$,

(vi) A ramified prime p is tamely ramified in $K/\mathbb{Q}$ if and only if $p|f(K)$ and $p^2 \nmid f(K)$.

Proof : (i) If $K \subset K_m$, then writing $f = f(K)$, and using Theorem 4.27 (v) we get $K \subset K_m \cap K_f = K_{(m,f)}$. Hence $f \leq (m, f) \leq f$ and $f(K)|m$ follows. The converse implication is obvious.

(ii) Since Theorem 4.27 (v) implies $K \cap L \subset K_{f(K)} \cap K_{f(L)} = K_{(f(K),f(L))}$, the assertion results from (i).

(iii) Write $f = f(KL)$. In view of $K \subset KL$, $L \subset KL$ and $KL \subset K_f$ we infer from (i) that f is divisible both by $f(K)$ and $f(L)$, so that $[f(K), f(L)]$ divides f. On the other hand, we have

$$KL \subset K_{f(K)}K_{f(L)} = KK_{[f(K),f(L)]}$$

and so (i) gives $f|[f(K), f(L)]$.

(iv) If $p \nmid f = f(K)$, then by Theorem 4.40 p does not ramify in $K_f/\mathbb{Q}$, and since $K \subset K_f$, it cannot ramify in $K/\mathbb{Q}$. If $p|f$ and p does not ramify in $K/\mathbb{Q}$, then write $f = p^a m$ with $a \geq 1$, $p \nmid m$, and observe that in view of Corollary 2 to Lemma 5.24, Theorem 4.40 and Corollary 1 to Proposition

6.2, p is unramified in $KK_m/\mathbb{Q}$. If $N = [KK_m : K]$, and P is any prime ideal above $p\mathbb{Z}$ in K_f, then, again using Theorem 4.40, we get

$$\begin{aligned}\varphi(p^a) &= e_{K_f/\mathbb{Q}}(P) = e_{K_f/KK_m}(P) \leq [K_f : KK_m] \\ &= [K_f : K_m]/N = \varphi(f)/\varphi(m)N = \varphi(p^a)/N.\end{aligned}$$

Thus $N = 1$ and $K \subset K_m$, contrary to the choice of f.

(v) Write again $f = f(K) = p^a m$ with $a \geq 0$, $p \nmid m$, and let P be a prime ideal lying above $p\mathbb{Z}$ in K_f. If $p|f$, $p^2 \nmid f$, then Theorem 4.40 shows that p does not divide $e_{K_f/\mathbb{Q}}(P)$, thus is tamely ramified in $K_f/\mathbb{Q}$, hence also in $K/\mathbb{Q}$. Conversely, if p is tamely ramified in $K/\mathbb{Q}$, then by (iv) we have $a \geq 1$, and by Corollary 2 to Lemma 5.30, Theorem 4.40 and Corollary 1 to Proposition 6.2 p is tamely ramified in $KK_{pm}/\mathbb{Q}$. Theorem 4.40 gives now

$$e_{K_f/\mathbb{Q}}(P) = \varphi(p^a) = p^{a-1}(p-1),$$

and we get $p^{a-1}|e_{K_f/KK_{pm}}(P)$. Writing $M = [KK_{pm} : K_{pm}]$ we obtain

$$\begin{aligned}p^{a-1}|e_{K_f/KK_{pm}}(P) \mid [K_f : KK_{pm}] &= [K_f : K_{pm}]/M \\ &= \varphi(f)/M\varphi(pm) = p^{a-1}/M.\end{aligned}$$

Thus $M = 1$ and we arrive at $K \subset K_{pm}$, which implies $f|pm$ and $p^2 \nmid f$. □

Corollary. *If $K/\mathbb{Q}$ is Abelian, then it has a normal integral basis if and only if it is tamely ramified.*

Proof: The necessity follows from Proposition 4.30 and Corollary 3 to Proposition 6.2. If $K/\mathbb{Q}$ is Abelian and tame, then (v) shows that $f(K)$ is squarefree, and the existence of a normal integral basis results from Proposition 4.31 and its corollary. □

It should be pointed out that one cannot expect equality in (ii), as the example $K = K_3$, $L = \mathbb{Q}(\sqrt{3})$ shows. Indeed, $f(K) = 3$, and since $d(L) = 12$ we get from (iv) that with certain positive a, b we have $f(L) = 2^a 3^b$ (actually $f(L) = 12$), and so $(f(K), f(L)) = 3$, However $K \cap L = \mathbb{Q}$ implies $f(K \cap L) = 1$.

2. Now we are going to determine the factorization of an arbitrary prime in an Abelian extension of $\mathbb{Q}$. According to Theorem 4.27 (ii) the Galois group of $K_m/\mathbb{Q}$ can be identified with the group $G(m)$ of residue classes (mod m), prime to m, a residue class a mod $m \in G(m)$ acting on K_m by $\zeta_m \mapsto \zeta_m^a$. If $K \subset K_m$, then, according to Galois theory, K corresponds to a subgroup H of $G(m)$. The following theorem shows that it is enough to know m and H to obtain factorization laws in K for every rational prime.

Theorem 8.2. *Let $K/\mathbb{Q}$ be Abelian, and let K_m be a cyclotomic field containing K. Denote by H the subgroup of $G(m)$ corresponding to K according to Galois theory. Then for every rational prime p we have*

$$pR_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e, \quad f_{K/\mathbb{Q}}(\mathfrak{P}_i) = f \quad (i = 1, 2, \ldots, g),$$

where the numbers e, f, g are determined as follows:

If $p \nmid m$ then $e = 1$, f equals the order of $p \bmod m$ in the factor group $G(m)/H$ and $g = [K : \mathbb{Q}]/ef$.

If $p|m$ then write $m = p^a m_1$ with $p \nmid m_1$, denote by N the number of residue classes $r \bmod m \in H$ satisfying $r \equiv 1 \pmod{m_1}$, and let N_1 be the number of residue classes $r \bmod m \in H$ for which $r \bmod m_1$ lies in the cyclic group generated by $p \bmod m_1$ in $G(m_1)$. Then

$$e = \varphi(p^a)/N, \quad f = FN/N_1, \quad g = [K : \mathbb{Q}]/ef,$$

where F is the order of $p \bmod m_1$ in $G(m_1)$.

Proof : We first determine the decomposition group, the inertia group and the first ramification group for an arbitrary prime ideal of K_m lying above p, and then apply Lemma 6.7 to descend to K. The first step is contained in the following lemma and the second is immediate.

Lemma 8.3. *Let $m = p^a m_1$ with $p \nmid m_1$, and let $\mathfrak{P}$ be a prime ideal of K_m lying above $p\mathbb{Z}$. The decomposition group $G_{-1}(\mathfrak{P})$ of $\mathfrak{P}$ consists of all residue classes $x \bmod m$ for which $x \bmod m_1$ lies in the cyclic group generated by $p \bmod m_1$, the inertia group of $\mathfrak{P}$ equals*

$$G_0(\mathfrak{P}) = \{x \bmod m : \ x \equiv 1 \pmod{m_1}\},$$

and the first ramification group $G_1(\mathfrak{P})$ is the maximal p-subgroup of $G_0(\mathfrak{P})$.

Proof : Assume first $a = 0$, i.e., $p \nmid m$, and let f be the order of $p \bmod m$ in $G(m)$. By Theorem 4.40 p is unramified and the degree of $\mathfrak{P}$ equals f. Thus by Proposition 6.8 the group $G_{-1}(\mathfrak{P})$ is cyclic of f elements. We show now that it contains the automorphism g_p, mapping ζ_m onto ζ_m^p, and this will confirm our first assertion in this case, since g_p is of order f. Observe that if $x = P(\zeta_m) \equiv 0 \pmod{\mathfrak{P}}$ (with $P \in \mathbb{Z}[t]$) then

$$0 \equiv P^p(\zeta_m) \equiv P(\zeta_m^p) \pmod{\mathfrak{P}},$$

and so $g_p(x) = P(\zeta_m^p) \in \mathfrak{P}$, i.e., $g_p \in G_{-1}(\mathfrak{P})$.

Now assume $m_1 = 1$, i.e., $m = p^a$ with non-zero a. In this case Theorem 4.40 yields $e_{K_m/\mathbb{Q}}(\mathfrak{P}) = \varphi(p^a)$ and $f_{K_m/\mathbb{Q}}(\mathfrak{P}) = 1$. Since $G_{-1}(\mathfrak{P})$ has $e_{K_m/\mathbb{Q}}(\mathfrak{P}) = [K_m : \mathbb{Q}]$ elements, it coincides with the full Galois group, and so our assertion about $G_{-1}(\mathfrak{P})$ is true also in this case.

In the general case observe that K_m is the composite of $L = K_{m_1}$ and $M = K_{p^a}$, and the Galois group $Gal(K_m/\mathbb{Q}) = G(m)$ is the product of

$Gal(L/\mathbb{Q}) = G(m_1)$ and $Gal(M/\mathbb{Q}) = G(p^a)$. These two factors are embedded in $Gal(K_m/\mathbb{Q})$ as follows: $Gal(L/\mathbb{Q})$ is the group fixing every element of M, and $Gal(M/\mathbb{Q})$ fixes every element of L. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the prime ideals of R_L and R_M lying below $\mathfrak{P}$, and let $g \in G_{-1}(\mathfrak{P})$. Write $g = [g_1, g_2]$ with $g_1 = g_{|L}$ and $g_2 = g_{|M}$. Note that $g_i(\mathfrak{p}_i)$ is conjugated with $\mathfrak{p}_i$ for $i = 1, 2$, and $g_i(\mathfrak{p}_i)R_{K_m} \subset g(\mathfrak{P}) = \mathfrak{P}$ implies $g_i(\mathfrak{p}_i) = \mathfrak{p}_i$, i.e., $g_i \in G_{-1}(\mathfrak{p}_i)$. This shows that $G_{-1}(\mathfrak{P})$ is contained in the product $G_{-1}(\mathfrak{p}_1) \times G_{-1}(\mathfrak{p}_2)$. Conversely, if for $i = 1, 2$ the elements g_i lie in $G_{-1}(\mathfrak{p}_i)$, then for $g = [g_1, g_2]$ we get $g(\mathfrak{P}) = \mathfrak{P}$. Indeed, if we had $g(\mathfrak{P}) = \mathfrak{Q} \neq \mathfrak{P}$ then $\mathfrak{p}_1 \subset \mathfrak{P}$ would imply $g_1(\mathfrak{p}_1) = g(\mathfrak{p}_1) \subset \mathfrak{Q}$ and thus $\mathfrak{P}\mathfrak{Q}$ would divide $\mathfrak{p}_1 R_{K_m}$. This is impossible because Theorem 4.40 implies that in the extension K_m/L the prime ideal factors of $p\mathbb{Z}$ are powers of prime ideals. Thus we arrive at the equality

$$G_{-1}(\mathfrak{P}) = G_{-1}(\mathfrak{p}_1) \times G_{-1}(\mathfrak{p}_2) = G_{-1}(\mathfrak{p}_1) \times Gal(M/\mathbb{Q}),$$

and it suffices to translate this result into the language of residue classes to obtain our first assertion in the general case.

To describe the group $G_0(\mathfrak{P})$ recall that according to Proposition 6.8 it corresponds to the maximal subfield of K_m in which p is unramified. Observe that this subfield equals $L = K_{m_1}$. In fact, Theorem 4.40 shows that p does not ramify in $L/\mathbb{Q}$ and since the equalities

$$[K_m : L] = \varphi(p^a) = e_{K_m/L}(\mathfrak{P}),$$

show that $f_{K_m/L}(\mathfrak{P}) = 1$, thus the corresponding $\mathfrak{p}$-adic extension is fully ramified. Hence p ramifies in every extension of $\mathbb{Q}$ containing L and contained in K_m. Consequently $G_0(\mathfrak{P})$ is the Galois group of K_m/L which can be identified with the set $\{r : g_r(\zeta_{m_1})\} = \zeta_{m_1}$. Now, in view of $\zeta_{m_1} = \zeta_m^p$ we get $g_r(\zeta_m) = \zeta_m^{rp}$, and this equals ζ_m if and only if $rp \equiv p \pmod{m}$, i.e., $r \equiv 1 \pmod{m_1}$, as asserted. Finally, the assertion concerning $G_1(\mathfrak{P})$ follows from Proposition 6.8. □

The theorem follows now immediately. □

Corollary 1. *If $K/\mathbb{Q}$ is Abelian of conductor f, then $P(K/\mathbb{Q})$ coincides with the set of all primes p with $p \bmod f \in H$.*

Proof: Apply the theorem with $m = f$, remembering that p lies in $P(K/\mathbb{Q})$ if and only if $e = f = 1$, and noting that by Proposition 8.1 (v) no prime from $P(K/\mathbb{Q})$ can divide f. □

Corollary 2. *If $K/\mathbb{Q}$ is Abelian of conductor f, then the map*

$$F : p \mapsto F_{K/\mathbb{Q}}(p),$$

defined for primes $p \nmid f$, induces an isomorphism of $G(f)/H$ onto $Gal(K/\mathbb{Q})$.

The existence of an isomorphism between these groups is immediate by Galois theory. The importance of this corollary lies in the fact that it provides an explicit isomorphism.

Proof : We first show that F induces a well-defined map from $G(f)/H$ onto $Gal(K/\mathbb{Q})$. To do that observe that if $p_i \bmod f$ $(i = 1, 2)$ lie in the same coset mod H, then by Theorem 7.29 (ii) $F_{K/\mathbb{Q}}(p_i)$ equals the restriction of $F_{K_f/\mathbb{Q}}(p_i)$ to K, and since $F_{K_f/\mathbb{Q}}(p_i) = p_i \bmod f$, $F_{K/\mathbb{Q}}(p_i)$ equals the coset mod H in which $p \bmod f$ lies. Thus $F_{K/\mathbb{Q}}(p_1) = F_{K/\mathbb{Q}}(p_2)$, showing that the map induced by F is well-defined. Its surjectivity results from Theorem 7.30. To show that it is a homomorphism it suffices to establish that if $p \equiv p_1 p_2 \pmod f$ then $F_{K/\mathbb{Q}}(p) = F_{K/\mathbb{Q}}(p_1) F_{K/\mathbb{Q}}(p_2)$, but this is obvious for $K = K_f$ and the general case follows by restriction to K. Now the assertion results from the observation that the injectivity of F is a consequence of the equality $\#G(f)/H = \#Gal(K/\mathbb{Q})$, which is a consequence of Galois theory. □

Corollary 3. *If m is a positive rational integer, and H is a subgroup of $G(m)$, then there exists an Abelian extension $K/\mathbb{Q}$ such that $P(K/\mathbb{Q})$ differs from the set of all primes p with $p \bmod m \in H$ by only finitely many primes.*

Proof : Let K be the subfield of K_m corresponding to H. An application of Corollary 1 shows that the two sets occurring in the assertion differ only by those primes which divide m, but not $f(K)$. □

The three corollaries proved above constitute a significant part of the class-field theory for Abelian extensions of $\mathbb{Q}$. Corollary 1 shows that every Abelian extension of $\mathbb{Q}$ is a class-field in the sense of H.Weber ([96b], [97]), and Corollary 2 is a form of Artin's Reciprocity Law for Abelian extensions of $\mathbb{Q}$. Corollary 3 is the Existence Theorem. The three statements have their analogues for Abelian extensions of any algebraic number field, belonging properly to class-field theory, which lies outside the scope of this book.

3. Let $K/\mathbb{Q}$ be Abelian and let $K \subset K_m$. As before denote by H the subgroup of $G(m)$ corresponding to K by Galois theory. Let $X(K)$ be the group of those characters of $G(m)$ which are equal to unity on H. Extend each of these characters first to a Dirichlet character mod m and then to a primitive character. For $\chi \in X(K)$ we shall denote by $f(\chi)$ its conductor, and by χ' the corresponding primitive Dirichlet character.

Note that if $X(K)$ and $X'(K)$ are the groups of characters associated with K, and corresponding to the embeddings of K into K_f (with $f = f(K)$) and into K_m, then every character of $X'(K)$ is lifted from a character of $X(K)$. This induces an isomorphism between $X(K)$ and $X'(K)$, which preserves conductors and the induced primitive characters. We may thus identify $X(K)$ and $X'(K)$. Under this convention the equality $X(K) = X(L)$ implies $K = L$.

Proposition 8.4. *For fixed m the map $K \mapsto X(K)$, defined for all subfields of K_m, induces a one-to-one correspondence between subfields of K_m and subgroups of the character group of $G(m)$. This map has the following properties:*

(i) $K \subset L$ holds if and only if $X(K) \subset X(L)$.

(ii) $X(K \cap L) = X(K) \cap X(L)$.

(iii) $X(KL)$ is the group generated by $X(K) \cup X(L)$.

(iv) $X(K) = G(m)$ holds if and only if $K = K_m$, and $X(K) = \{1\}$ holds if and only if $K = \mathbb{Q}$.

(v) $\#X(K) = [K : \mathbb{Q}]$.

Proof : This is simply a restatement of the fundamental theorem of Galois theory for K_m in terms of characters. □

Proposition 8.5. *Let K be an Abelian field. If K is real, then all characters of $X(K)$ are even, and if K is complex, then $X(K)$ contains the same number of odd and even characters. In this case the even characters form a subgroup of $X(K)$ equal to $X(K^+)$, with K^+ being the maximal real subfield of K.*

Proof : Since the element $\tau = -1 \bmod m$ of $G(m)$ acts as complex conjugation, the field K will be real if and only if τ acts on K trivially, i.e., -1 lies in H, and this occurs if and only if all characters of $X(K)$ are even. This argument shows also that if K is complex, then $X(K)$ contains at least one odd character. Since in this case even characters form a subgroup X' of index 2 in $X(K)$, we see that $X(K)$ contains the same number of even and odd characters. As X' is the maximal subgroup of $X(K)$ consisting of even characters, the first part of our proposition jointly with Proposition 8.4 show that $X' = X(K^+)$. □

4. Now we are going to utilize the group $X(K)$ to express the Dedekind zeta-function of an Abelian field as a product of Dirichlet's L-functions. This important formula will be later used to derive an explicit formula for the class-number of Abelian fields, and also for the proof of the Siegel-Brauer theorem in the Abelian case.

Theorem 8.6. *If $K/\mathbb{Q}$ is Abelian then*

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(s, \chi'),$$

where χ' is the primitive Dirichlet character induced by χ.

Proof : Since both sides of the asserted equality are meromorphic, it suffices to establish it for s in the half-plane Re $s > 1$. In that plane we have

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p} \text{ over } p} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

and

$$\prod_{\chi \in X(K)} L(s, \chi') = \prod_p \prod_{\chi \in X(K)} \frac{1}{1 - \chi'(p)p^{-s}},$$

(where p runs over all rational primes, and we have $\chi'(p) = 0$ for primes p dividing the conductor of χ), the two products being absolutely convergent. To prove the theorem it is enough to establish the equality

$$\prod_{\mathfrak{p} \text{ over } p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{\chi \in X(K)} \frac{1}{1 - \chi'(p)p^{-s}} \tag{8.1}$$

for every prime p. To prove it observe first that if

$$pR_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$$

and $f = f_{K/\mathbb{Q}}(\mathfrak{p}_i)$ $(i = 1, 2, \ldots, g)$, then the left-hand side of (8.1) is equal to $(1 - p^{-fs})^{-g}$. We shall show that the right-hand side of (8.1) has the same value. We start with the case $p \nmid m$. In this case we have $e = 1$. If $\chi \in X(K)$ then χ' equals unity on H, and since Theorem 8.2 shows that f equals the order of $p \bmod m$ in $G(m)/H$, we get $\chi'(p)^f = \chi'(p^f) = 1$, hence all possible values of $\chi'(p)$ are f-th roots of unity. Moreover, if A is the group of characters of $G(m)/H$ which are equal to 1 on the coset mod H determined by $p \bmod m$, then the set of characters χ' which attain at p a fixed f-th root of unity forms a coset $\bmod A$ in the group of all characters of G/H. It follows that this set has $\#(G/H)f^{-1}$ elements and we can write

$$1 - \chi'(p)p^{-s} = \prod_{j=0}^{f} (1 - \zeta_f^j p^{-s})^g.$$

Now note that for all x we have

$$\prod_{j=0}^{f} (1 - \zeta_f^j x)^g = 1 - x^f,$$

and putting here $x = p^{-s}$ we obtain

$$\prod_{j=0}^{f} (1 - \zeta_f^j p^{-s})^g = 1 - p^{-fs},$$

and

$$\prod_{\chi} (1 - \chi'(p)p^{-s}) = (1 - p^{-fs})^g,$$

implying (8.1).

If $p|m$, then write $m = p^a m_1$ with $p \nmid m_1$. It follows from Proposition 8.1 that $L = K \cap K_{m_1}$ is the maximal subfield of K in which p remains unramified, and Proposition 6.7 implies that if $\mathfrak{p}$ is a prime ideal of R_L lying over p, then $f_{L/\mathbb{Q}}(\mathfrak{p}) = f$ and $g_{L/\mathbb{Q}}(\mathfrak{p}) = g$.

Since $p|f(\chi)$ implies $\chi'(p) = 0$, we have

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = \prod_{\substack{\chi \in X(K) \\ f(\chi)|m_1}} (1 - \chi'(p)p^{-s}).$$

But $f(\chi)|m_1$ holds if and only if $\chi \in X(K_m)$, and so

$$\{\chi \in X(K) : \ f(\chi)|m_1\} = X(K) \cap X(K_{m_1}) = X(L)$$

by Proposition 8.4 (ii). It follows that

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = \prod_{\chi \in X(L)} (1 - \chi'(p)p^{-s}),$$

and in view of $p \nmid m_1$ the application of the case already considered leads to

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = (1 - p^{-f's})^{g'},$$

with $f' = f_{L/\mathbb{Q}}(\mathfrak{p})$ and $g' = g_{L/\mathbb{Q}}(\mathfrak{p})$. But we have already shown that $f' = f$ and $g' = g$, hence (8.1) results also in this case. □

Our next result expresses the discriminant and the conductor of an Abelian field in terms of the associated character group.

Proposition 8.7. *If $K/\mathbb{Q}$ is Abelian then*

$$d(K) = (-1)^u \prod_{\chi \in X(K)} f(\chi),$$

where u denotes the number of odd characters in $X(K)$, and

$$f(K) = LCM\{f(\chi) : \ \chi \in X(K)\}.$$

Proof : The preceding theorem implies

$$1 = \frac{\zeta_K(1-s)}{\zeta_K(s)} \prod_{\chi \in X(K)} \frac{L(s,\chi')}{L(1-s,\chi')} = \frac{\zeta_K(1-s)}{\zeta_K(s)} \prod_{\chi \in X(K)} \frac{L(s,\chi')}{L(1-s,\overline{\chi}')}.$$

If K is real, then using Theorem 7.3, Proposition 8.5 and Corollary 2 to Proposition 7.12 we arrive at

$$1 = |d(K)|^{1/2-\sigma} \prod_{\chi \in X(K)} f(\chi)^{\sigma - 1/2} \tag{8.2}$$

with $\sigma = \mathrm{Re}\, s$. Putting $\sigma = 0$, and using Proposition 2.15 we get the first assertion in this case.

If K is complex then the same approach leads to

$$1 = 2^{\alpha}\pi^{\beta}\left(|d(K)|^{-1}\prod_{\chi\in X(K)} f(\chi)\right)^{\sigma-1/2}\left(\frac{\Gamma(1-s)\Gamma(s/2)\Gamma((1+s)/2)}{\Gamma(s)\Gamma((1-s)/2)\Gamma(1-s/2)}\right)^{r_2},$$

where $\alpha = -r_2(1-2\sigma)$ and $\beta = r_2(\sigma-1)$. Using the formula

$$\Gamma(s)\Gamma(s+1/2) = \sqrt{\pi}2^{1-2s}\Gamma(2s)$$

we again get (8.2), and the first assertion results as in the previous case.

To obtain the second assertion embed K into K_f (with $f = f(K)$), and observe that for χ in $X(K)$ we have $f(\chi)|f$. Thus $f' = LCM\{f(\chi:\ \chi\in X(K)\}$ divides f. Since every character of $X(K)$ can be regarded as a character $\mathrm{mod}\, f'$, we get $K\subset K_{f'}$ and so $f|f'$, hence $f' = f$ follows. □

Corollary. *We have*

$$\prod_{\substack{\chi\in X(K)\\ \chi\neq 1}} |\tau(\chi')| = \sqrt{|d(K)|}.$$

Proof: The equality $|\tau(\chi')| = \sqrt{f(\chi)}$ results from Corollary 2 to Proposition 6.15, and so the assertion follows from the first part of the proposition. □

5. The results just presented permit us to determine arithmetic properties of an Abelian field in a rather quick way, provided we know its conductor f and its position in the lattice of subfields of K_f. To illustrate this let us consider the subfields of the field K_{13}. Since 13 is a prime, the group $Gal(K_{13}/\mathbb{Q}) = G(13)$ is cyclic of order 12, and has the following subgroups: $H_1 = G(13)$, $H_2 = \{1,3,4,9,10,12\}$, $H_3 = \{1,5,8,12\}$, $H_4 = \{1,3,9\}$, $H_6 = \{1,12\}$ and $H_{12} = \{1\}$ (here we denote the residue m mod 13 simply by m). Accordingly we have five fields of conductor 13. Let L_r be the field corresponding to H_r ($r = 1,2,3,4,6,12$). Obviously we have $[L_r:\mathbb{Q}] = r$, and in particular $L_1 = \mathbb{Q}$. Proposition 8.7 gives for the remaining fields the equality $d(L_r) = (-1)^{u_r}13^{a_r}$, where u_r is the number of odd characters equal to unity on H_r, and

$$a_r + 1 = \#X(L_r) = \#(G(13)/H_r) = 12/\#H_r = [L_r:\mathbb{Q}] = r.$$

Since 2 is a primitive root mod 13, every character of $G(13)$ is determined by its value at 2, and we obtain easily a complete list of these characters (we invite the reader to prepare such a list by himself) from which it follows that $u_2 = u_3 = u_6 = 0$, $u_4 = 2$, $u_{12} = 6$. Thus the fields L_2, L_3 and L_6 are real,

whereas L_4 and L_{12} are complex. In all cases the discriminant is positive, and we get $d(L_r) = 13^{r-1}$ for all r.

The factorization of rational primes in L_r results immediately from Theorem 8.2. The only ramified prime is $p = 13$, and we get $13R_L = \mathfrak{p}_r^r$ for all r, whereas for other primes we get

$$pR_{L_r} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

with $g = r/t$, t being the least positive integer for which $p^t \bmod 13 \in H_r$.

To conclude this example let us determine explicitly the fields involved. Clearly $L_{12} = K_{13}$ and $L_2 = \mathbb{Q}(\sqrt{13})$, since L_2 is a quadratic field of discriminant 13. As the maximal real subfield of K_{13} is of degree 6, it must be equal to L_6. Thus $L_6 = \mathbb{Q}(\cos(2\pi/13))$. This leaves us with L_3 and L_4. Observe that every element $x \in K_{13}$ can be written in the form

$$x = \sum_{j=1}^{12} A_j \zeta^j \quad (A_j \in \mathbb{Q})$$

(where $\zeta = \zeta_{13}$) in a unique way. We have $x \in L_r$ if and only if $A_j = A_{js \bmod 13}$ for every j and every $s \in H_r$. Consequently $\omega_1 = \zeta + \zeta^5 + \zeta^8 + \zeta^{12}$ lies in $L_3 \setminus \mathbb{Q}$, hence generates L_3. It follows from Theorem 2.20 that x is integral if and only if all A_j's lie in $\mathbb{Z}$, and we see that an integral basis of L_3 is provided by ω_1, $\omega_2 = \zeta^2 + \zeta^3 + \zeta^{10} + \zeta^{11}$ and $\omega_3 = \zeta^4 + \zeta^6 + \zeta^7 + \zeta^9$.

A similar argument shows that the numbers

$$w_1 = \zeta + \zeta^3 + \zeta^9, \quad w_2 = \zeta^2 + \zeta^5 + \zeta^6$$
$$w_3 = \zeta^4 + \zeta^{10} + \zeta^{12}, \quad w_4 = \zeta^7 + \zeta^8 + \zeta^{11}$$

form an integral basis of L_4. Since $L_4^+ = \mathbb{Q}$ and w_1 is non-real, it generates L_4. We leave to the reader the dull task of obtaining minimal polynomials for the generators of L_3 and L_4.

6. Now we may obtain information on asymptotic properties of Abelian extensions $K/\mathbb{Q}$ with a given Galois group and $f(K) \leq x$.

We shall do this in a slightly more general setting. Let k be a fixed field, and let for each rational integer $N \geq 1$ an extension L_N/K be given, which is assumed to be finite and Abelian. Denote by $A(N)$ the Galois group of L_N/k.

The family $\{L_N\}$ will be called *multiplicative* if it satisfies the following two conditions:

(i) For all M, N we have $L_M L_N = L_{[M,N]}$ and $L_M \cap L_N = L_{(M,N)}$.

(ii) If $(M, N) = 1$ then $A(MN) \sim A(M) \times A(N)$.

Note that if $k = \mathbb{Q}$ and L_N is the N-th cyclotomic field, then by Theorem 4.27 the family $\{L_N\}$ is multiplicative.

We shall consider also the family $\mathcal{F}$ of all extensions K/k satisfying $K \subset K_N$ for a suitable N depending on K. For a given Abelian group A let $N_A(x)$ be defined as the number of all fields $K \in \mathcal{F}$ which satisfy $Gal(K/k) \sim A$, and which are contained in a suitable field L_N with $N \leq x$. If $k = \mathbb{Q}$ and L_N is the N-th cyclotomic field, then $N_A(x)$ counts fields with Galois group A and conductor not exceeding x.

We prove now that under certain restrictions on $A(q)$ for prime powers q one can obtain an asymptotic formula for $N_A(x)$.

Theorem 8.8. *Let $\{L_N\}$ be a multiplicative family of finite Abelian extensions of a field k, and let A be a fixed finite Abelian group of order $\neq 1$. For any finite Abelian group H let $n_H(N)$ be the number of homomorphisms of $A(N)$ into H. Assume further that for every subgroup B of A there exist non-negative constants $a(B)$ and $c(B)$ such that for every prime power q the inequality*

$$n_B(q) \leq c(B) \tag{8.3}$$

holds, and for all complex s with Re $s > 1$ *one has*

$$\sum_p \frac{n_B(p)}{p^s} = a(B) \log \frac{1}{s-1} + g(s), \tag{8.4}$$

with p running over all rational primes, and $g(s) = g_B(s)$ being regular in the closed half-plane Re $s \geq 1$. *Assume finally that for every proper subgroup B of A the inequality*

$$a(B) < a(A) \tag{8.5}$$

is satisfied.

Then for x tending to infinity we have

$$N_A(x) = (C(A) + o(1)) x \log^{a(A)-2} x$$

with a positive constant $C(A)$.

Proof : Observe first that for fixed B the function $n_B(N)$ is multiplicative. The condition (8.3) shows that the series

$$F_B(s) = \sum_{N=1}^{\infty} n_B(N) N^{-s}$$

converges absolutely and almost uniformly in the half-plane Re $s > 1$, and we can expand its sum into an Euler product

$$F_B(s) = \prod_p \left(1 + \sum_{j=1}^{\infty} n_B(p^j) p^{-js} \right).$$

Since (8.3) ensures that $F_B(s)$ can vanish only at zeros of those factors of the Euler product which correspond to primes not exceeding $1 + c(B)$, we can write for Re $s > 1$

$$F_B(s) = g_1(s) \exp\left(\sum_p n_B(p) p^{-s}\right),$$

with g_1 regular for Re $s \geq 1$ and $g_1(1) \neq 0$.

The condition (8.4) leads now to the equality

$$F_B(s) = \frac{g_2(s)}{(s-1)^{a(B)}}, \tag{8.6}$$

valid for Re $s > 1$ with g_2 regular for Re $s \geq 1$ and not vanishing at $s = 1$.

For a group H let $m_H(N)$ be the number of surjective homomorphisms of $A(N)$ onto H. Then obviously

$$\sum_{H \subset B} m_H(N) = n_B(N),$$

with H ranging over all subgroups of B. This relation permits us to calculate $m_H(N)$ in view of the following lemma of Delsarte [48], which is an analogue of the Möbius inversion formula:

Lemma 8.9. *To every pair $B \subset A$ of finite Abelian groups one can assign a rational integer $t(A, B)$, so that whenever f, g are complex-valued functions defined in the set of all subgroups of a finite Abelian group G, satisfying*

$$f(A) = \sum_{B \subset A} g(B) \quad (A \subset G),$$

then

$$g(A) = \sum_{B \subset A} t(A, B) f(B).$$

One has in particular $t(A, A) = 1$.

Proof : Let $\{1\} = H_1, H_2, \ldots, H_r = A$ be all subgroups of a group $A \subset G$, ordered in such a way that $H_i \subset H_j$ implies $i \leq j$ (but not necessarily conversely) and put

$$\epsilon(i, j) = \begin{cases} 1 & \text{if } H_i \subset H_j, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\epsilon(i, i) = 1$, and for $i > j$ we have $\epsilon(i, j) = 0$, the matrix $[\epsilon(i, j)]$ is invertible, and its inverse $[e(i, j)]$ satisfies

$$e(i, j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } j > i. \end{cases}$$

Moreover, for $j = 1, 2, \ldots, r$ we have

$$f(H_j) = \sum_{i=1}^{j} \epsilon(i,j) g(H_i),$$

and

$$g(H_j) = \sum_{i=1}^{j} e(i,j) f(H_i) \quad (j = 1, 2, \ldots, r).$$

Putting here $j = r$ and $t(H_r, H_i) = e(i,r)$ we get the assertion. □

The lemma implies

$$m_B(N) = \sum_{G \subset B} t(B,G) n_G(N),$$

and this leads to the equality

$$\sum_{N=1}^{\infty} m_A(N) N^{-s} = F_A(s) + \sum_{\substack{A \\ B \neq A}} t(A,B) F_B(s),$$

holding for Re $s > 1$. Using (8.5) and (8.6) we get with a certain r the equality

$$\sum_{N=1}^{\infty} m_A(N) N^{-s} = \frac{g_2(s)}{(s-1)^{a(A)}} + \sum_{j=1}^{r} \frac{h_j(s)}{(s-1)^{t_j}},$$

where $t_1, \ldots, t_r$ are real numbers smaller than $a(A)$, and $h_1, \ldots, h_h$ are functions regular in the half-plane Re $s \geq 1$.

The kernel of a homomorphism counted by m_A corresponds by Galois theory to a field K satisfying

$$k \subset K \subset L_N \quad \text{and} \quad Gal(K/k) \sim A. \tag{8.7}$$

If $V(A)$ denotes the number of automorphisms of A, then to every field K satisfying (8.7) there correspond $V(A)$ different homomorphisms counted by $m_A(N)$. This shows that if $c_A(N)$ denotes the number of such fields K, then

$$c_A(N) = m_A(N)/V(A).$$

Finally, let $b_A(N)$ be the number of fields K satisfying (8.7), but not contained in L_M for any proper divisor M of N. Our assumptions imply that if $K \subset L_M$ and $K \subset L_N$, then $K \subset L_{(M,N)}$, hence every field counted by $c_A(N)$ is counted by $b_A(d)$ for exactly one divisor d of N.

This gives

$$\sum_{d|N} b_A(d) = c_A(N),$$

hence Möbius inversion formula implies

$$b_A(N) = \sum_{d|N} \mu(N/d) c_A(d),$$

and we arrive at the equality

$$\sum_{N=1}^{\infty} b_A(N) N^{-s} = \zeta^{-1}(s) \sum_{N=1}^{\infty} c_A(N) N^{-s}$$
$$= \frac{1}{V(A)} \left(\frac{g_2(s)}{(s-1)^{1-a(A)}} + \sum_{j=1}^{r} \frac{h_j(s)}{(s-1)^{t_j}} \right),$$

valid for Re $s > 1$. Note that our assumptions imply $a(A) > 1$. Indeed, for $B = \{1\}$ we have $n_B(p) = 1$ for all primes p, and (8.5) gives $a(A) > a(B) = 1$. We may thus invoke Theorem I of Appendix II to obtain the asserted formula. □

Corollary 1. *If A is a finite Abelian group, then the number of extensions $K/\mathbb{Q}$ with Galois group A and $f(K) \leq x$ equals*

$$(C(A) + o(1)) x \log^{a(A)-2} x,$$

with $C(A) > 0$ and

$$a(A) = \sum_{d|\#A} \frac{r_A(d)}{\varphi(d)},$$

where $r_A(d)$ is the number of elements of order d in A.

Proof : We apply the theorem with $k = \mathbb{Q}$ and $L_N = K_N$, the N-th cyclotomic field. Condition (8.3) follows from the fact that in this case the group $A(q)$ has for prime-powers q at most two generators. Moreover one sees easily that for prime p and every finite Abelian group B the equality

$$n_B(p) = \sum_{d|p-1} r_B(d)$$

holds. Therefore using Corollary 6 to Proposition 7.16 (applied to $K = \mathbb{Q}$) we get

$$\sum_p n_B(p) p^{-s} = \sum_{d|\#B} r_B(d) \sum_{p \equiv 1 \pmod{d}} p^{-s} = a(B) \log \frac{1}{s-1} + g(s),$$

with

$$a(B) = \sum_{d|\#B} r_B(d)/\varphi(d),$$

and a function g regular in Re $s > 1$. This establishes (8.4).

It remains to verify (8.5), but this is immediate, because if B is a proper subgroup of A, then for at least one value of d dividing $\#A$ we must have $r_B(d) < r_A(d)$. Thus all assumptions of the theorem are satisfied and the assertion follows. □

In certain cases one can deduce from the last corollary asymptotic results for the number of fields with a given Galois group and bounded discriminant. We can see this on the example of cyclic fields of prime degree:

Corollary 2. *The number of cyclic extensions of $\mathbb{Q}$ of a prime degree p and $|d(K)| \leq x$ equals $(C + o(1))x^{\alpha}$ with $\alpha = 1/(p-1)$ and $C = C(p) > 0$.*

Proof : If $K/\mathbb{Q}$ is cyclic of degree p, then the associated group $X(K)$ of characters contains $p-1$ non-trivial characters, all of the same conductor f, because each of them generates $X(K)$, and if χ_1 is a power of χ_2, then $f(\chi_1)|f(\chi_2)$. Proposition 8.7 gives now $|d(K)| = f^{p-1}$ and $f(K) = f$, and so the conditions $|d(K)| \leq x$ and $f(K) \leq x^{\alpha}$ are equivalent. The assertion follows now from Corollary 1. □

8.2. The Class-number Formula and the Siegel-Brauer Theorem

1. In this section we express the class-number of an Abelian extension $K/\mathbb{Q}$ in terms of the values of L-functions associated with characters from $X(K)$ and other invariants of K. Then we shall prove the Siegel-Brauer theorem concerning the asymptotic behaviour of the product $h(K)R(K)$ for Abelian fields.

Theorem 8.10. *If $K/\mathbb{Q}$ is Abelian, and $w(K)$ denotes the number of roots of unity contained in K, then*

$$h(K) = \frac{w(K)\sqrt{|d(K)|}}{2^{r_1+r_2}\pi^{r_2}R(K)} \prod_{\substack{\chi \in X(K) \\ \chi \neq 1}} L(1, \chi'),$$

where χ' is the primitive Dirichlet character associated with χ.

Proof : By Theorem 8.6 we have

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(1, \chi').$$

Comparing the residues at $s = 1$, using Theorem 7.3, and noting that for the principal character χ_0 we have $L(s, \chi_0') = \zeta(s)$ we obtain the assertion. □

Corollary 1. *If $m \not\equiv 2 \pmod 4$, then for the m-th cyclotomic field K_m we have*

$$h(K_m)R(K_m) = \frac{\epsilon_m \sqrt{|d(K_m)|}}{(2\pi)^{\varphi(m)/2}} \prod_{\chi \neq \chi_0} L(1, \chi'),$$

where

$$\epsilon_m = \begin{cases} 1 & \text{if } m \text{ is even,} \\ 2 & \text{if } m \text{ is odd,} \end{cases}$$

and χ runs over nonprincipal characters mod$m$.

Proof : Follows directly from Corollary to Theorem 4.27 and Theorems 8.10 and 4.17. □

Corollary 2. *If K is a quadratic field of discriminant d, and w is the number of roots of unity contained in K, then*

$$h(K) = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L_d(1) & \text{if } d < 0, \\ \frac{\sqrt{d}}{2 \log \epsilon} L_d(1) & \text{if } d > 0, \end{cases}$$

where $L_d(s) = L(s, \chi_d)$ is the L-function associated with Kronecker's extension $\chi_d(x) = \left(\frac{d}{x}\right)$ of the Legendre symbol, and, in case of positive d, $\epsilon > 1$ is the fundamental unit of K.

Proof : In view of the theorem it suffices to establish that the primitive character induced by the unique non-trivial character $\chi \in X(K)$ equals χ_d. Since $\#X(K) = [K : \mathbb{Q}] = 2$, χ is real, Proposition 8.7 gives $\operatorname{sgn} d = \chi(-1)$ and $f(\chi) = |d|$. Thus χ' is a real primitive character mod $|d|$ satisfying $\chi'(-1) = \operatorname{sgn} d$.

By Proposition 6.13 we may write

$$d = \operatorname{sgn} d \cdot p_1^a p_2 \cdots p_r$$

with $p_1 = 2$, $p_2, \ldots, p_r$ being odd primes and $a = 0, 2$ or 3. Proposition 6.10 shows that $\chi' = \chi_1 \cdots \chi_r$, where each χ_i is a real primitive character mod 2^a for $i = 1$ and mod p_i for $i \geq 2$. Thus for $i = 2, 3, \ldots, r$ we have $\chi_i(x) = \left(\frac{x}{p_i}\right)$. If $a = 0$, then the equality $\chi' = \chi_d$ follows immediately. If $a = 2$, then $\chi_1(x)$ equals $(-1)^{(x-1)/2}$, the unique primitive character mod 4. In the case $a = 3$ we have a choice, as there are two primitive characters mod 8, namely $(-1)^{(x^2-1)/8}$ and $(-1)^{(x^2-1)/8+(x-1)/2}$, but the condition $\chi'(-1) = \operatorname{sgn} d$ determines χ_1 uniquely also in this case. It is immediate that in all cases χ' equals the symbol of Kronecker[4]. □

[4] The reader not acquainted with Kronecker's symbol may take the above construction for its definition.

For a positive integer n let K_n^+ be the maximal real subfield of the n-th cyclotomic field K_n. The class-number $h(K_n^+)$ is denoted by h_n^+, and called usually *the second factor* of $h(K_n)$, whereas the ratio $h(K_n)/h_n^+$ is denoted by h_n^-, and called the *first factor* of $h(K_n)$.

Corollary 3. *If p is an odd prime then*

$$h_p^+ = \frac{p^{(p-3)/4}}{R(K_p)} \prod_{\chi \text{ even}} L(1,\chi),$$

and

$$h_p^- = \frac{p^{(p+3)/4}}{2^{(p-3)/2}\pi^{(p-1)/2}} \prod_{\chi \text{ odd}} L(1,\chi),$$

both products taken over non-principal characters mod p.

Proof : Since $K_p/\mathbb{Q}$ is cyclic, Theorem 3.21 shows that there is a fundamental system of units lying in K_p^+, where it forms a system of fundamental units. This implies the equality

$$R(K_p) = 2^{(p-3)/2} R(K_p^+).$$

Since $w(K_p^+) = 2$, and Proposition 8.7 gives $|d(K_p^+)| = p^{(p-3)/2}$, the formula for the second factor results. Applying Corollary 1, and dividing the obtained expression by h_p^+, we get the formula for the first factor. □

2. The first factor h_p^- is always an integer. This was first noted by Kummer [50a]. We present a proof due to Kronecker [63]:

Proposition 8.11. *If p is an odd prime, then the canonical homomorphism of $H(K_p^+)$ into $H(K_p)$ is injective, and $h(K_p) = h_p^+ h_p^-$ is a factorization into integers.*

Proof : Write $L = K_p$, $L^+ = K_p^+$ and let I be an ideal in R_{L^+} such that IR_L is principal. In view of Proposition 4.46 (i) it suffices to show that I is principal itself. Write $IR_L = aR_L$ and observe that $\overline{I} = I$ implies $\overline{a} = ua$ with a suitable unit u of L. By Corollary to Theorem 3.21 we can write $u = \zeta u_1$ with $u_1 \in U(L^+)$, and a root of unity $\zeta \in E(L)$. From

$$|a| = |\overline{a}| = |\zeta u_1 a| = |u_1 a|$$

we get $|u_1| = 1$, hence $u_1 = \pm 1$. Thus $\overline{a} = \zeta' a$ with $\zeta' \in E(L)$. By Corollary to Theorem 4.27 we can write $\zeta' = \pm\zeta_p^m$ with a suitable integer m. This gives $\overline{a} = \pm\zeta_p^m a$. Let s be a solution of the congruence $2s \equiv m \pmod{p}$ and put $b = \zeta_p^s a$. Then

$$\overline{b} = \zeta_p^{-s}\overline{a} = \pm\zeta_p^{m-s} a = \pm\zeta_p^s a = \pm b,$$

and $IR_L = bR_L$. If $b = \bar{b}$ then $b \in L^+$ and so I is principal.

It remains to show that the equality $\bar{b} = -b$ is impossible. Let $\pi = 1 - \zeta_p$. By Corollary to Theorem 4.40 π generates a prime ideal in R_L, and so we may write $b = \pi^r c$ with $(cR_L, \pi R_L) = 1$ and a suitable $r \geq 0$. Since by the same corollary one has

$$pR_L = (\pi R_L)^{p-1}, \quad f_{L/\mathbb{Q}}(\pi R_L) = 1,$$

we get $pR_{L^+} = \mathfrak{p}^{(p-1)/2}$ with a suitable prime ideal $\mathfrak{p}$. Thus $\mathfrak{p}R_L = (\pi R_L)^2$, and it follows that r must be even, say, $r = 2t$. This leads to

$$-\pi^{2t}c = -b = \bar{b} = \overline{\pi}^{2t}\bar{c} = \pi^{2t}\zeta_p^{-2t}\bar{c}$$

and $\bar{c} = -\zeta_p^{2t}c$, and finally $\bar{c} \equiv -c \pmod{\pi}$ because of $\zeta_p \equiv 1 \pmod{\pi}$. This congruence is impossible, because if we write

$$c = \sum_{j=0}^{p-2} A_j \zeta_p^j$$

with $A_j \in \mathbb{Z}$, then $c \equiv \sum_{j=0}^{p-2} A_j \equiv \bar{c} \equiv -c \pmod{\pi}$ and thus $2c \equiv 0 \pmod{\pi}$, which is excluded by our choice of c. □

3. The class-number formula given in Theorem 8.10 contains values of Dirichlet's L-functions at $s = 1$. We express now these values by finite sums of elementary functions.

Proposition 8.12. *If $m \geq 3$, and χ is a primitive character* mod m, *then*

$$L(1, \chi) = -\frac{\tau(\chi)}{m} \sum_{j=1}^{m-1} \overline{\chi(j)} \left(\log\left(2 \sin \frac{\pi j}{m}\right) - i\frac{\pi j}{m} \right).$$

If moreover χ is odd, then

$$L(1, \chi) = i\pi \frac{\tau(\chi)}{m^2} \sum_{x=1}^{m-1} x\overline{\chi(x)}.$$

Proof : For $|x| < 1$ define

$$f(x) = \sum_{n=1}^{\infty} \chi(n) \frac{x^n}{n}.$$

Since the series defining $L(s, \chi)$ converges at $s = 1$ (the sum $\sum_{n \leq x} \chi(n)$ being bounded by m and the sequence $1/n$ decreasing to zero), we have

$$\lim_{x \to 1} f(x) = L(1, \chi).$$

Now

$$f(x) = \sum_{r=1}^{m-1} \chi(r) \sum_{n \equiv r \pmod m} \frac{x^n}{n} = \sum_{r=1}^{m-1} \chi(r) \sum_{n=0}^{\infty} \frac{x^{r+mn}}{r+mn}.$$

Hence

$$f'(x) = -\frac{\sum_{r=1}^{m-1} \chi(r) x^{r-1}}{x^m - 1},$$

and in view of $f(0) = 0$ we obtain

$$f(x) = -\int_0^x \sum_{r=1}^{m-1} \chi(r) \frac{t^{r-1}}{t^m - 1} dt.$$

The integrand can be written in the form

$$\sum_{j=0}^{m-1} \frac{a_j}{t - \zeta_m^j},$$

where the a_j's are complex constants, which can be determined by the following calculation:

Write

$$\sum_{r=1}^{m-1} \chi(r) t^{r-1} = \sum_{j=0}^{m-1} a_j \frac{t^m - 1}{t - \zeta_m^j},$$

and put $t = \zeta_m^k$ for $k = 0, 1, \ldots, m-1$. This gives

$$\sum_{r=1}^{m-1} \chi(r) \zeta_m^{kr-1} = a_k m \zeta_m^{k(m-1)} = a_k m \zeta_m^{-k},$$

thus $a_k = \tau_k(\chi)/m$, where

$$\tau_k(\chi) = \sum_{r=1}^{m-1} \chi(r) \zeta_m^{kr}.$$

Finally we get

$$L(1, \chi) = -\frac{1}{m} \int_0^1 \sum_{j=0}^{m-1} \frac{\tau_j(\chi)}{t - \zeta_m^j} dt. \tag{8.8}$$

A direct computation shows that

$$\int_0^1 \frac{dt}{t - \zeta_m^j} = \log\left(2 \sin \frac{\pi j}{m}\right) + i\pi \left(\frac{1}{2} - \frac{j}{m}\right),$$

thus the first assertion follows from Proposition 6.9 (i) and the following lemma:

Lemma 8.13. *If χ is a primitive Dirichlet character* mod m *and* $(j,m) > 1$, *then* $\tau_j(\chi) = 0$.

Proof : Write $m_1 = (j,m)$, $k = m/m_1$ and choose an integer a prime to m, satisfying $a \equiv 1 \,(\mathrm{mod}\ k)$ and $\chi(a) \neq 1$. If there were no such integer, then $m = f(\chi)$ would divide k, thus $(j,m) = 1$, contrary to our assumption. Now

$$\tau_j(\chi) = \sum_{r=1}^{m-1} \chi(ar)\zeta_m^{arj} = \chi(a) \sum_{r=1}^{m-1} \chi(r)\zeta_m^{arj} = \chi(a)\tau_j(\chi),$$

because ζ_m^j is a primitive k-th root of unity, $ar \equiv r \,(\mathrm{mod}\ k)$, and thus $\zeta_m^{arj} = \zeta_m^{rj}$. Finally we see that $\tau_j(\chi)$ vanishes, as asserted. □

To obtain the second assertion note that if χ is odd then $\overline{\chi}(m-x) = \overline{\chi}(-x) = -\overline{\chi}(x)$, thus

$$\sum_{j=1}^{m-1} \overline{\chi}(j) \log\left(2\sin\frac{\pi j}{m}\right)$$
$$= \frac{1}{2}\sum_{j=1}^{m-1}\left(\overline{\chi}(j)\log\left(2\sin\frac{\pi j}{m}\right) + \overline{\chi}(m-j)\log\left(2\sin\frac{\pi(m-j)}{m}\right)\right) = 0.$$

□

Corollary 1. (Dirichlet's class number formula) *If K is a quadratic number field of discriminant d, w is the number of roots of unity in K, $\epsilon > 1$ is the fundamental unit of K in case $d > 0$, and $\chi_d(n) = \left(\frac{d}{j}\right)$, then*

$$h(K) = \begin{cases} -\frac{w}{2|d|}\sum_{j=1}^{|d|}\chi_d(j)j & \text{if } d < 0, \\ -\frac{1}{\log\epsilon}\sum_{0<j<d/2}\chi_d(j)\log\left(\sin\frac{\pi j}{d}\right) & \text{if } d > 0. \end{cases}$$

Proof : For $d < 0$ Proposition 8.5 shows that χ_d is odd. Using Theorem 6.16 we get

$$L(1,\chi_d) = \mathrm{Re}\ L(1,\chi_d) = -\frac{1}{|d|^{3/2}}\sum_{j=1}^{|d|} j\chi_d(j),$$

and it suffices to apply Corollary 2 to Theorem 8.10.

For positive d we obtain

$$L(1,\chi_d) = \mathrm{Re}\ L(1,\chi_d) = -\frac{1}{\sqrt{d}}\sum_{j=1}^{d-1}\chi_d(j)\log\left(2\sin\frac{\pi j}{d}\right)$$
$$= -\frac{1}{\sqrt{d}}\sum_{j=1}^{d-1}\chi_d(j)\log\left(\sin\frac{\pi j}{d}\right).$$

Since by Proposition 8.5 χ_d is even, we have $\chi_d(d-j) = \chi_d(j)$, and it remains to apply Corollary 2 to Theorem 8.10. □

Our second application of Proposition 8.12 is an upper bound for h_p^-.

Corollary 2. *If p is an odd prime then*

$$h_p^- < 2p\left(\frac{p}{24}\right)^{(p-1)/4}.$$

Proof : The proposition and Corollary 2 to Theorem 8.10 imply

$$h_p^- = \frac{p^{(p+3)/4}}{2^{(p-3)/2}p^{p-1}} \prod_{\chi \text{ odd}} |\tau(\chi)\sum_{j=1}^{p-1} j\overline{\chi}(j)|,$$

and since Corollary 4 to Proposition 8.7 implies

$$\prod_{\chi \text{ odd}} |\tau(\chi)| = |d(K_p)/d(K_p^+)|^{1/2},$$

we get

$$h_p^- = \frac{1}{(2p)^{(p-3)/2}} \prod_{\chi \text{ odd}} |\sum_{j=1}^{p-1} j\overline{\chi}(j)|.$$

It remains to evaluate the product occurring in the last equality. Since

$$\sum_{\chi \text{ odd}} \chi(m)\overline{\chi}(n) = \begin{cases} (p-1)/2 & \text{if } p \nmid mn, m \equiv \ \ n \pmod p, \\ -(p-1)/2 & \text{if } p \nmid mn, m \equiv -n \pmod p, \\ 0 & \text{in other cases,} \end{cases}$$

we get

$$\sum_{\chi \text{ odd}} |\sum_{j=1}^{p-1} \overline{\chi}(j)j|^2 = \sum_{\chi \text{ odd}} \sum_{x,y=1}^{p-1} \overline{\chi}(x)\chi(y)xy$$

$$= \sum_{j=1}^{p-1} \left(\sum_{x\equiv y\equiv j \pmod p} xy(p-1) - \sum_{x\equiv -y\equiv j \pmod p} xy(p-1)/2 \right)$$

$$= \frac{p-1}{2}\left(\sum_{j=1}^{p-1} j^2 - \sum_{j=1}^{p-1} j(p-j)\right) = \frac{p(p-1)^2(p-2)}{12}.$$

Applying the inequality between the arithmetic and geometric means we arrive finally at

$$\sum_{\chi odd} |\sum_{j=1}^{p-1} \overline{\chi}(j) j|^{4/(p-1)} \leq \frac{p(p-1)(p-2)}{6} \leq \frac{p^3}{6},$$

and this leads to

$$h_p^- < \frac{1}{(2p)^{(p-3)/2}} \left(\frac{p^3}{6}\right)^{(p-1)/4} = 2p \left(\frac{p}{24}\right)^{(p-1)/4}. \qquad \square$$

4. Now we shall be concerned with the asymptotic behaviour of the product $h(K)R(K)$ for Abelian extensions $K/\mathbb{Q}$. An upper estimate is provided by Corollary 4 to Theorem 7.3, which implies,

$$\limsup \frac{\log(h(K)R(K)}{\log|d(K)|} \leq \frac{1}{2}$$

when K runs over all fields of a fixed degree, arranged according to the absolute value of the discriminant. In the sequel we shall always assume tacitly that any considered sequence of fields is arranged in this way.

The Siegel-Brauer theorem, which we now shall prove for Abelian extensions, states that in this relation lim sup can be replaced by lim and the inequality by equality.

Theorem 8.14. *If K runs over all Abelian extensions of $\mathbb{Q}$ having a fixed degree n, then*

$$\lim \frac{\log(h(K)R(K))}{\log|d(K)|} = \frac{1}{2}.$$

Proof : We start with a lower bound for the residue of $\zeta_K(s)$:

Lemma 8.15. *There is a constant $B = B(n) > e^{-13n} > 0$ such that for every field K of degree n over the rationals and every s_0 with $0 < s_0 < 1$, the inequality $\zeta_K(s_0) \leq 0$ implies*

$$h(K)\kappa(K) \geq B s_0(1-s_0)|d(K)|^{s_0-1}.$$

Proof : Corollary 1 to Theorem 7.3 shows that the inequality $\zeta_K(s_0) \leq 0$ implies

$$\int_{V(x)\geq 1} \left(\hat{f}(x)V(x)^{s_0} + f(x)V(x)^{1-s_0}\right) dm_I(x)$$
$$\leq h(K)\kappa(K)\left(\frac{1}{s_0\sqrt{|d(K)|}} + \frac{1}{1-s_0}\right) \leq \frac{h(K)\kappa(K)}{s_0(1-s_0)}, \tag{8.9}$$

where $f = \prod_v f_v$ is the function used in the proof of Theorem 7.3. It was shown in the proof of that theorem that for v Archimedean we have $\hat{f}_v =$

f_v, whereas for v non-Archimedean the function $\hat{f}_v$ is the product of the characteristic function of D_v^{-1} and $N(D_v)^{-1/2}$, $D_v = \pi_v^M R_v$ (where π_v is a fixed generator of the prime ideal $\mathfrak{p}_v$ of R_v) being the different of the corresponding local extension.

Since f and $\hat{f}$ are both non-negative, (8.9) leads to

$$\begin{aligned} h(K)\kappa(K) \geq & s_0(1-s_0)\int_{V(x)\geq 1} \hat{f}(x)V(x)^{s_0}dm_I(x) \\ \geq & \ s_0(1-s_0)\int_{\prod_v P_v} \hat{f}(x)V(x)^{s_0}dm_I(x) \\ = & \ s_0(1-s_0)\prod_v \int_{P_v} \hat{f}_v(x_v)v(x_v)^{s_0}d\mu_v^*(x) \\ = & \ s_0(1-s_0)\prod_v I_v, \end{aligned} \tag{8.10}$$

where

$$P_v = \begin{cases} \{x_v : \ v(x_v) \geq 1\} & \text{if } v \text{ is non-Archimedean,} \\ \{x_v : \ 1 \leq v(x_v) \leq 2\} & \text{if } v \text{ is Archimedean.} \end{cases}$$

We estimate now the integrals I_v from below. In the non-Archimedean case we have

$$\begin{aligned} I_v = & \frac{1}{\sqrt{N(D_v)}}\int_{D_v^{-1}\cap P_v} v(x_v)^{s_0}d\mu_v^*(x) \\ = & \frac{1}{\sqrt{N(D_v)}}\sum_{m=-M}^{0}\int_{\pi_v^m U_v} v(x_v)^{s_0}d\mu_v^*(x) \\ \geq & \ \frac{1}{\sqrt{N(D_v)}}\int_{\pi_v^{-M}U_v} v(x_v)^{s_0}d\mu_v^*(x). \end{aligned}$$

This leads to

$$I_v \geq \frac{1}{\sqrt{N(D_v)}}N(\mathfrak{p}_v)^{Ms_0}\int_{\pi_v^{-M}U_v} d\mu_v^*(x) = N(D_v)^{s_0-1}.$$

If v is real then we get

$$\begin{aligned} I_v = \int_1^2 \exp(-\pi x^2)x^{s_0}\frac{dx}{x} \geq & \ e^{-4\pi}\int_1^2 \frac{dx}{x} \\ = & \ e^{-4\pi}\log 2, \end{aligned}$$

and if v is complex then

$$\begin{aligned} I_v = & 2\iint_S \exp(-2\pi(y_1^2+y_2^2))(y_1^2+y_2^2)^{s_0-1}dy_1dy_2 \\ \geq & \ 2\exp(-4\pi)\int_0^{2\pi} d\varphi \int_1^{\sqrt{2}} r^{2s_0}\frac{dr}{r} = 2\pi e^{-4\pi}\log 2, \end{aligned}$$

where $S = \{(y_1, y_2) \in \mathbb{R}^2 : \ 1 \leq y_1^2 + y_2^2 \leq 2\}$.

This implies

$$\prod_v I_v \geq B \prod_{v \notin S_\infty} N(D_v)^{s_0-1} = B|d(K)|^{s_0-1},$$

where

$$B = B(n) = \inf_{r_1+2r_2=n} \{(2\pi)^{r_2}(e^{-4\pi}\log 2)^{r_1+r_2}\} > e^{-13n},$$

and this jointly with (8.10) proves the lemma. □

From this lemma one can deduce an old result of Hecke, dealing with the class-number of imaginary quadratic fields:

Corollary. *To every $a \in (0, 1/2)$ there corresponds an effective constant $c(a) > 0$ with the property that if K is an imaginary quadratic field of discriminant $d < -4$ such that $\zeta_K(s)$ has no real zeros in the interval $[1-a/\log|d|, 1)$, then*

$$h(K) \geq c(a)\frac{\sqrt{|d|}}{\log|d|}.$$

Proof : Put $k = |d|$. The assumptions imply $\zeta_K(1 - a/\log k) < 0$, so we may apply the lemma with $s_0 = 1 - a/\log k$. This gives

$$h\kappa \geq e^{-26}\left(1 - \frac{a}{\log k}\right)\frac{a}{\log k}k^{a/\log k} \geq \frac{ae^{a-26}}{2\log k},$$

and since $\kappa = \pi/\sqrt{|d(K)|}$, the assertion follows. □

Our next lemma gives an upper bound for the value of Dirichlet L-functions at $s = 1$.

Lemma 8.16. *If $m \geq 3$, and χ is a non-principal character* mod m, *then*

$$|L(1,\chi)| \leq 2 + \log m < 3\log m.$$

Proof : For $N > m$ we have

$$\begin{aligned}
&|\sum_{n=1}^{N}\frac{\chi(n)}{n}| \\
&= |\sum_{n=1}^{m}\frac{\chi(n)}{n} + \frac{1}{N}\sum_{n=1+m}^{N}\chi(n) + \sum_{r=1+m}^{N-1}\left(\frac{1}{r} - \frac{1}{r+1}\right)\sum_{n=1+m}^{M}\chi(n)| \\
&\leq \sum_{n=1}^{m}\frac{1}{n} + \frac{m}{N} + \sum_{r=1+m}^{N-1} m\left(\frac{1}{r} - \frac{1}{r+1}\right) \\
&= \sum_{n=1}^{m}\frac{1}{n} + \frac{m}{m+1} \leq \log m + 2 < 3\log m. \qquad \square
\end{aligned}$$

Utilizing the two preceding lemmas we can now give a lower bound for the residue $h(K)\kappa(K)$ of $\zeta_K(s)$. This will be achieved by a suitable choice of the parameter s_0 in Lemma 8.15.

Lemma 8.17. *To each positive ϵ there corresponds a positive constant $B_1 = B_1(n,\epsilon)$, such that for every Abelian extension $K/\mathbb{Q}$ of degree n one has*

$$h(K)\kappa(K) \geq B_1|d(K)|^{-\epsilon}.$$

Proof : We may freely assume that $0 < \epsilon < 1/2$. Suppose first that for all Abelian extensions $K/\mathbb{Q}$ of degree n we have $\zeta_K(s) \neq 0$ for $1 - \epsilon/2n < s < 1$. Since Corollary 1 to Theorem 7.3 implies that $\zeta_K(s)$ is negative in some interval $(1-\alpha, 1)$, the inequality

$$\zeta_K(1 - \epsilon/2n) \leq 0$$

results for our fields. Applying Lemma 8.15 with $s_0 = 1 - \epsilon/2n$ we get

$$h(K)\kappa(K) \gg |d(K)|^{-\epsilon/2n} \gg |d(K)|^{-\epsilon},$$

and the proof is complete.

Now assume that there is an Abelian extension $K_0/\mathbb{Q}$ of degree n such that ζ_K vanishes at a point s_0 of the interval $(1 - \epsilon/2n, 1)$. Fix such s_0, let $K/\mathbb{Q}$ be an arbitrary Abelian extension of degree n, and put $L = KK_0$. The field L is obviously Abelian and we have $[L : \mathbb{Q}] \leq n^2$. Let K_m be a cyclotomic field containing L, and let H_0, H_1 and H_2 be the subgroups of its Galois group corresponding to K_0, K and L, respectively. Finally for $i = 0, 1, 2$ denote by A_i the set of characters mod m which are trivial on H_i, and, as before, let χ' be the primitive character induced by a character χ. According to Theorem 8.6 we can write

$$\zeta_L(s) = \prod_{\chi \in A_2} L(s, \chi'),$$
$$\zeta_{K_0}(s) = \prod_{\chi \in A_0} L(s, \chi'),$$

and this together with $A_2 \supset A_0$ implies $\zeta_L(s_0) = 0$. We can now apply Lemma 8.15, which yields

$$h(L)\kappa(L) \geq B' s_0(1 - s_0)|d(L)|^{s_0 - 1},$$

with $B' = \min_{m \leq n^2} B(m)$.

Corollary 2 to Proposition 6.2 gives

$$|d(L)| \leq |d(K_0)d(K)|^n,$$

and we obtain

$$h(K)\kappa(K) \geq B_2|d(K)|^{n(s_0-1)} \geq B_3|d(K)|^{-\epsilon/2},$$

with B_2 and B_3 depending on n, ϵ and s_0. In view of the equality

$$h(K)\kappa(K) = h(L)\kappa(L) \prod_{\chi \in A_2 \setminus A_1} L(1,\chi')^{-1}$$

we can write

$$h(K)\kappa(K) \geq |d(K)|^{-\epsilon/2} \prod_{\chi \in A_2 \setminus A_1} L(1,\chi')^{-1}.$$

Lemma 8.16 gives now

$$\prod_{\chi \in A_2 \setminus A_1} L(1,\chi') \leq B_4 \prod_{\chi \in A_2 \setminus A_1} \log f(\chi) \leq B_5 \prod_{\chi \in A_2 \setminus A_1} f(\chi)^{\epsilon/2},$$

and finally we arrive at

$$h(K)\kappa(K) \geq B_6|d(K)|^{-\epsilon/2} \prod_{\chi \in A_2 \setminus A_1} f(\chi)^{-\epsilon/2} \geq B_7|d(K)|^{-\epsilon},$$

since in view of Proposition 8.7 we have

$$\prod_{\chi \in A_2 \setminus A_1} f(\chi) = |d(L)/d(K)|. \qquad \square$$

The last lemma shows that

$$\log h(K)R(K) \geq \log\left(|d(K)|^{1/2-\epsilon}\right) + O(1),$$

and now it suffices to apply Corollary 4 to Theorem 7.3 to obtain the assertion of the theorem. $\square$

Corollary 1. *For imaginary quadratic fields K we have*

$$\log h(K) = \left(\frac{1}{2} + o(1)\right) \log |d(K)|,$$

for $|d(K)|$ tending to infinity.

Proof : In this case we have $R(K) = 1$. $\square$

Corollary 2. *There are only finitely many imaginary quadratic fields with unique factorization.*

Proof : Apply Theorem 1.45 and the preceding corollary. $\square$

The last corollary is not effective, and does not lead to an explicit bound for the largest absolute value of the discriminant of an imaginary quadratic field with unique factorization. An effective proof of this corollary will be given in the last section of this chapter.

Corollary 3. *When K runs over all complex Abelian fields of a fixed degree n, then the ratio $h^-(K) = h(K)/h(K^+)$ tends to infinity. More precisely,*

$$\liminf \frac{\log h^-(K)}{\log |d(K)|} \geq \frac{1}{4}.$$

Proof : Proposition 3.20 implies that any fundamental system of units of K^+ generates a subgroup of finite index in $U(K)$. This shows that the regulator R' of such system, taken in K, is not smaller than $R(K)$, according to Corollary 2 (iii) to Theorem 3.13. Since obviously $R' = 2^r R(K^+)$, with $r = n/2 - 1$, this leads to

$$\log R(K) \leq r \log 2 + \log R(K^+), \tag{8.11}$$

and thus

$$\log h^-(K) \geq \log(h(K)R(K)) - \log(h(K^+)R(K^+)).$$

Let now $\epsilon > 0$ be fixed. It follows from the theorem that if $|d(K^+)|$ is sufficiently large, say $|d(K^+)| \geq T$, then

$$\log(h(K)R(K)) \geq (1/2 - \epsilon) \log |d(K)| \geq (1 - 2\epsilon) \log |d(K^+)|,$$

and

$$\log(h(K^+)R(K^+)) \leq (1/2 - \epsilon) \log |d(K^+)|.$$

(We used here the inequality $|d(K)| \geq |d(K^+)|^2$, resulting from Corollary 1 to Proposition 4.15.)

Subtracting, we get

$$\log(h(K^+)R(K^+)) \geq (1/2 - 3\epsilon) \log |d(K^+)| \geq (1/4 - 3\epsilon/2) \log |d(K)|,$$

hence it remains to consider those fields K for which $|d(K^+)| \leq T$. By Theorem 2.24 this gives only finitely many possibilities for K^+. Thus $R(K^+)$ lies between two positive constants, and (8.11) gives $R(K) = O(1)$. By Theorem 8.14 we have

$$\log h(K) = (1/2 + o(1) \log |d(K)| - \log R(K).$$

If $R(K) \geq 1$, then $\log R(K) = O(1)$, and if $R(K) < 1$, then $\log R(K)$ is negative, thus in both cases we get

$$\log h(K) \geq (1/2 + o(1)) \log |d(K)|,$$

and as in our case $1 \leq h(K^+) = O(1)$, we are done. □

Corollary 4. *There are only finitely many complex Abelian fields with given degree and class-number.* □

8.3. Class-number of Quadratic Fields

1. The problem of determining the class-number of quadratic fields goes back to Gauss [01], who actually considered the number of equivalence classes of *binary quadratic forms* $aX^2+2bXY+cY^2$ with rational integral coefficients a, b, c, satisfying $(a, b, c) = 1$, and having a fixed determinant $b^2 - ac$, under the action of $SL_2(\mathbb{Z})$. Those two class-numbers are intimately connected, as we shall see in this subsection. However, in contrast to Gauss, we shall consider binary quadratic forms $f(X, Y) = aX^2+bXY+cY^2$ with $a, b, c \in \mathbb{Z}$, satisfying $(a, b, c) = 1$. Such forms are called *primitive*. The discriminant $d(f)$ of f is defined by $d(f) = b^2 - 4ac$.

A matrix

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in SL_2(\mathbb{Z})$$

(i.e., a matrix with entries from $\mathbb{Z}$ and unit discriminant) acts on f by means of

$$Mf = g(X, Y) = f(AX + BY, CX + DY).$$

Since the forms f and Mf have the same discriminant, and the inverse M^{-1} also lies in $SL_2(\mathbb{Z})$, we obtain a partition of the set of all primitive quadratic forms of the same discriminant into classes, each class consisting of equivalent forms, two forms being considered equivalent if there is a matrix in $SL_2(\mathbb{Z})$ mapping one of them into the other.

The theorem, which we now prove, establishes a connection between the number of equivalence classes of forms and the class number of a quadratic number field.

Theorem 8.18. *Let K be a quadratic number field of discriminant d, and let I be a non-zero ideal of R_K. Denoting the conjugate of an element $c \in K$ by c' choose a $\mathbb{Z}$-basis a_1, a_2 of I in such a way that the number $a_1a_2' - a_2a_1'$ is either positive, or lies on the upper half of the imaginary axis. With I we associate the quadratic form*

$$f_I(X, Y) = \frac{N_{K/\mathbb{Q}}(a_1X + a_2Y)}{N(I)} = \frac{(a_1X + a_2Y)(a_1'X + a_2'Y)}{N(I)}.$$

We assert:

(i) The form f_I has integral rational coefficients, it is primitive, its discriminant equals d, and in the case of $d < 0$ it is positive definite.

(ii) The map $I \mapsto f_I$ of the set of all non-zero ideals of R_K into the set of all primitive quadratic forms with coefficients in $\mathbb{Z}$ and of discriminant d (which, in case $d < 0$, are positive definite) is surjective.

(iii) If two ideals I, J lie in the same class of $H^*(K)$, then the forms f_I and f_J are equivalent. Conversely, if f_I, f_J are equivalent forms, then the ideals I, J lie in the same class.

Proof : Fix the generator $\sqrt{d}$ of K so that it is either positive, or lies on the upper half of the imaginary axis. It follows from Propositions 2.9 (ii) and 2.13 that if $1, \omega$ form an integral basis of K, and $a_1 = A_{11} + A_{12}\omega$, $a_2 = A_{21} + A_{22}\omega$ (with $A_{ij} \in \mathbb{Z}$), then $N(I) = |\det[A_{ij}]|$, and an easy computation with the use of Theorem 2.18 shows that $a_1 a_2' - a_1' a_2 = \pm N(I)\sqrt{d}$. Changing, if necessary, the sign of a_1 we can find a basis of I of the required form. Now note that the coefficients of f_I are equal to $N_{K/\mathbb{Q}}(a_1)/N(I)$, $(a_1 a_2' + a_1' a_2)/N(I)$ and $N_{K/\mathbb{Q}}(a_2))/N(I)$, respectively. Since a_1, a_2 lie in I we get $N(I)|N_{K/\mathbb{Q}}(a_i)$, and we see that $a_1 a_2' + a_1' a_2$ is a rational integer lying in $II' = N(I)R_K$, hence it is divisible by $N(I)$. This shows that the coefficients of f_I are rational integers. Note also that the discriminant of f_I equals d, and this implies that our form is primitive. Indeed, if there is a prime p such that the form f_I/p has integral coefficients, then its discriminant D equals d/p^2, thus $p = 2$. However, every discriminant of a quadratic form is congruent either to 0 or to 1 mod 4, hence $d(f_I) = 4D$ with $D \equiv 0, 1 \pmod 4$, which is obviously impossible. To obtain the last part of (i) it suffices to observe that in the case of negative d the coefficient of X^2 in f_I is positive.

To prove (ii) consider a primitive binary quadratic form $F(X, Y) = AX^2 + BXY + CY^2$ with discriminant d, and assume that F is positive definite in case of negative d. Put

$$I = \begin{cases} (B + \sqrt{d})\mathbb{Z} + 2C\mathbb{Z} & \text{if } C > 0, \\ (B - \sqrt{d})\mathbb{Z} + 2C\mathbb{Z} & \text{if } C < 0. \end{cases}$$

Note that the case $C = 0$ cannot arise, as then d would be a square. An easy check shows now that I is an ideal, satisfying $f_I = F$, and this proves (ii).

Assume now that the ideals $I = a_1\mathbb{Z} + a_2\mathbb{Z}$ and $J = b_1\mathbb{Z} + b_2\mathbb{Z}$ lie in the same class of $H^*(K)$, and let c_1, c_2 be totally positive elements of R_K such that $c_1 I = c_2 J$ holds. Then $c_1 a_1, c_1 a_2$ and $c_2 b_1, c_2 b_2$ are two bases of the ideal $c_1 I$, thus there exists a matrix $M = [m_{ij}] \in GL_2(\mathbb{Z})$ with

$$c_1 a_i = m_{i1} c_2 b_1 + m_{i2} c_2 b_2 \quad (i = 1, 2). \tag{8.12}$$

To the ideal $c_1 I$ there corresponds, via the basis $c_1 a_1, c_1 a_2$, the form

$$F(X, Y) = \frac{N_{K/\mathbb{Q}}(c_1 a_1 X + c_1 a_2 Y)}{N(I) N_{K/\mathbb{Q}}(c_1)},$$

and, via the basis $c_2 b_1, c_2 b_2$, the form

$$G(X, Y) = \frac{N_{K/\mathbb{Q}}(c_2 b_1 X + c_2 b_2 Y)}{N(J) N_{K/\mathbb{Q}}(c_2)}.$$

Since evidently $F = f_I$, $G = f_J$ and $G = MF$, we have $f_J = M g_I$ and so it suffices to show that $\det M = 1$. Now

$$\begin{aligned} c_2b_1c_2'b_2' - c_2'b_1'c_2b_2 &= N(c_2J)\sqrt{d} = N(c_1I)\sqrt{d} = c_1a_1c_1'a_2' - c_1'a_1'c_1a_2 \\ &= (m_{11}c_2b_1 + m_{12}c_2b_2)(m_{21}c_2'b_1' + m_{22}c_2'b_2') \\ &- (m_{11}c_2'b_1' + m_{12}c_2'b_2')(m_{21}c_2b_1 + m_{22}c_2b_2) \\ &= (c_2b_1c_2'b_2' - c_2'b_1'c_2b_2)\det M, \end{aligned}$$

and this shows that indeed $\det M = 1$.

Finally we prove that equivalent forms correspond to ideals from the same class in $H^*(K)$. Let F and G be two forms associated with ideals $I = a_1\mathbb{Z} + a_2\mathbb{Z}$ and $J = b_1\mathbb{Z} + b_2\mathbb{Z}$, respectively, and assume that F and G are equivalent, i.e., for a certain matrix $M = [m_{ij}] \in SL_2(\mathbb{Z})$ we have

$$G(X,Y) = F(m_{11}X + m_{12}Y, m_{21}X + m_{22}Y).$$

Comparing the coefficients we see that either b_1/b_2 or $(b_1/b_2)'$ equals

$$(a_1m_{11} + a_2m_{21})/(a_1m_{12} + a_2m_{22}),$$

since these numbers differ only in sign from the solutions of the equation $G(1,x) = 0$.

Observe that the second case is impossible. Indeed, in this case we would have, with a suitable $t \in R_K$, the equalities

$$a_1m_{11} + a_2m_{21} = tb_1', \quad a_1m_{12} + a_2m_{22} = tb_2',$$

and so

$$(b_1b_2' - b_1'b_2)N_{K/\mathbb{Q}}(t) = -(a_1a_2' - a_1'a_2)\det M = -(a_1a_2' - a_1'a_2),$$

showing that $N_{K/\mathbb{Q}}(t)$ is negative. But on the other hand

$$G(X,Y) = \frac{N_{K/\mathbb{Q}}(tb_1'X + tb_2'Y)}{N(I)} = \frac{N_{K/\mathbb{Q}}(t)N(J)G(X,Y)}{N(I)},$$

whence $N_{K/\mathbb{Q}}(t) = N(I)/N(J)$ must be positive, a contradiction.

Hence the first case must hold, and so with a suitable $t \in K$ we have

$$a_1m_{11} + a_2m_{21} = tb_1, \quad a_1m_{12} + a_2m_{22} = tb_2,$$

and the preceding argument gives $N_{K/\mathbb{Q}}(t) > 0$. Since $\det M = 1$, we see that $tb_1\mathbb{Z} + tb_2\mathbb{Z} = I$, thus $tJ = I$, and so I and J lie in the same class in $H^*(K)$, because t is either totally positive, or totally negative, and the latter case can be avoided by changing the signs of a_1 and a_2, which change does not affect the argument. □

2. Using Theorem 8.18, and results concerning the reduction of binary quadratic forms one can determine the value of $h^*(K)$, and obtain upper bounds for it (see e.g. Narkiewicz [86, Chap. 5]). However, using Corollary 2 to Theorem 8.10 one can obtain in the case of real K much better bounds, and this is what we now show. To simplify the notation we shall write $h(d)$ to denote $h(K)$, whenever K is the quadratic field of discriminant d.

Proposition 8.19. *For positive d one has $h(d) < \sqrt{d}$.*

The proof will be based on a lemma of Hua, which improves in this case Lemma 8.16:

Lemma 8.20. *If $d > 0$, then*

$$L_d(1) < 1 + \frac{1}{2}\log d.$$

(Let us recall that $L_d(s) = L(s, \chi_d)$, where $\chi_d(n) = \left(\frac{n}{d}\right)$.)

Proof : Consider the function $S(n)$ defined for positive integers n by

$$S(n) = \sum_{a=1}^{n} \sum_{m=1}^{a} \chi_d(m)$$

and put $S(-1) = S(0) = 0$. In view of the identity

$$S(n) - 2S(n-1) + S(n-2) = \chi_d(n) \quad (n = 1, 2, \ldots)$$

we may write

$$L_d(1) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n} = 2\sum_{n=1}^{\infty} \frac{S(n)}{n(n+1)(n+2)}.$$

Now put $A = [\sqrt{d}] + 1$, and split the last sum into two: S_1, with n ranging from 1 to $A - 1$, and S_2, in which n runs from A to infinity. Since $|S(n)| \leq n(n+1)/2$, we get

$$|S_1| \leq \sum_{n=1}^{A-1} \frac{1}{n+2} \leq \log(1 + A) - \log 2 \leq \log \sqrt{d}.$$

To evaluate S_2 we prove first for $j \geq \sqrt{d}$ the inequality

$$|S(j)| \leq j\sqrt{d}/2. \tag{8.13}$$

In view of $\chi_d(-n) = \chi_d(n)$ we obtain

$$\sqrt{d}S(j) = \sqrt{d}\sum_{a=0}^{j}\sum_{n=1}^{a}\chi_d(n) = \frac{\sqrt{d}}{2}\sum_{a=0}^{j}\sum_{n=-a}^{a}\chi_d(n).$$

Theorem 6.16 combined with Proposition 6.14 (i) gives the equality

$$\chi_d(n)\sqrt{d} = \sum_{x=1}^{d}\chi_d(x)\exp(2\pi ixn/d)$$

(which holds also in the case $(d,n) > 1$, both sides being 0), hence

$$\begin{aligned}\sqrt{d}S(j) &= \frac{1}{2}\sum_{a=0}^{j}\sum_{n=-a}^{a}\sum_{x=1}^{d}\chi_d(x)\exp(2\pi ixn/d)\\ &= \frac{1}{2}\sum_{x=1}^{d}\chi_d(x)\sum_{a=0}^{j}\sum_{n=-a}^{a}\exp(2\pi ixn/d),\end{aligned}$$

implying

$$|\sqrt{d}S(j)| \le \frac{1}{2}\sum_{x=1}^{d}|\sum_{a=0}^{j}\sum_{n=-a}^{a}\exp(2\pi ixn/d)|.$$

In view of the identity

$$\sum_{a=0}^{j}\sum_{n=-1}^{a}\exp(itn) = \left(\frac{\sin(t(j+1)/2)}{\sin(t/2)}\right)^2$$

holding for real $t \neq 2\pi m$ ($m \in \mathbb{Z}$), we get, with j' denoting the least non-negative residue of j mod d,

$$\begin{aligned}&\sum_{x=1}^{d}|\sum_{a=0}^{j}\sum_{n=-a}^{a}\exp(2\pi ixn/d)| = \sum_{x=1}^{d}\left(\frac{\sin(\pi x(j+1)/d)}{\sin(\pi x/d)}\right)^2\\ &= \sum_{x=1}^{d}\left(\frac{\sin(\pi x(j'+1)/d)}{\sin(\pi x/d)}\right)^2 = \sum_{x=1}^{d}\sum_{a=0}^{j'}\sum_{n=-1}^{a}\exp(2\pi ixn/d)\\ &= \sum_{a=0}^{j'}\sum_{n=-a}^{a}\sum_{x=1}^{d}\exp(2\pi ixn/d) = (j'+1)d - (j'+1)^2.\end{aligned}$$

This leads to

$$|S(j)| \le \frac{1}{2}(1+j')(\sqrt{d} - (j'+1)/\sqrt{d}). \tag{8.14}$$

Now, if $\sqrt{d} \le j < d$, then $j' = j$, and $\frac{1}{2}(1+j)\sqrt{d} - \frac{1}{2}(j+1)^2/\sqrt{d}$ does not exceed $j\sqrt{d}/2$, which implies (8.13) in this case. In the case $j > d$ we obtain from (8.14) by trivial estimate the inequality

$$|S(j)| \leq \frac{1}{2}(1+d)\sqrt{d} \leq j\sqrt{d}/2,$$

which again gives (8.13). Finally

$$|S(d)| = |S(d-1)| \leq (d-1)\sqrt{d}/2.$$

Inequality (8.13) being established, we can now conclude the proof. In fact, that inequality implies

$$|S_2| \leq \sqrt{d} \sum_{j=A}^{\infty} \frac{j+1}{j+2} = \frac{\sqrt{d}}{A+1} < 1,$$

and this shows

$$|S| \leq |S_1| + |S_2| \leq 1 + \log\sqrt{d},$$

as required. □

Proof of Proposition 8.19: We use Corollary 2 to Theorem 8.10. The required evaluation of $L_d(1)$ is provided by the lemma just proved, and we need only to obtain a convenient estimate of $\log\epsilon$ from below. For this purpose write ϵ in the form

$$\epsilon = \frac{T + U\sqrt{d}}{2}$$

with $T, U \in \mathbb{Z}$ and $T^2 - dU^2 = \pm 4$. It is clear that

$$T^2 = dU^2 \pm 4 \geq (d-4)U^2,$$

whence $T \geq U\sqrt{d-4}$ and

$$\epsilon > \frac{U(\sqrt{d} + \sqrt{d-4})}{2} \geq \sqrt{d-3},$$

hence $\log\epsilon > \log(d-3)/2$. This evaluation suits our purpose, because for $d \geq 17$ we get

$$h(d) = \frac{\sqrt{d}L_d(1)}{2\log\epsilon} \leq \sqrt{d}\frac{1 + \frac{1}{2}\log d}{\log(d-3)} < \sqrt{d},$$

and it remains to observe that for $d < 17$ we have $h(d) = 1$. Indeed, otherwise by Lemma 3.8 there would exist a non-principal ideal of norm not exceeding $\sqrt{d}/2$. However, if $d < 17$ is a discriminant, then $d \leq 13$ and so the only ideal in question is the unit ideal, obviously principal. □

3. A lower bound for $h(d)$ is provided for negative d by Theorem 8.14, which implies $h(d) > d^{1/2-\delta}$ for every positive δ and sufficiently large $|d|$. No comparable result is known for positive d, and in fact it has been conjectured that for infinitely many $d > 0$ one has $h(d) = 1$. We shall now give a lower bound valid for infinitely many positive discriminants, which is a particular case of the Ankeny-Brauer-Chowla theorem:

Theorem 8.21. *For every positive δ one can find infinitely many real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $h(d) > d^{1/2-\delta}$.*

Proof: Fix $\delta > 0$ and let $\epsilon(d) > 1$ be the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$. By Theorem 8.14 we have

$$h(d) > \frac{d^{1/2-\delta}}{\log \epsilon(d)}$$

for all sufficiently large d. We have thus to bound $\epsilon(d)$ from above, and every bound of the form $\log \epsilon(d) = O(\log d)$, valid for infinitely many fields, will do.

We need an elementary result first:

Lemma 8.22. *For infinitely many n the number $n^2 + 1$ is square-free.*

Proof: Observe first that $n^2 + 1$ is never divisible by 4. For an odd prime p let $A_p(T)$ be the number of integers $n \leq T$ for which $n^2 + 1$ is divisible by p^2, and observe that the number $A(T)$ of integers $n \leq T$ for which $n^2 + 1$ is square-free satisfies

$$A(T) \geq T - \sum_{3 \leq p \leq T} A_p(T).$$

Obviously we have

$$A_p(T) = \sum_{\substack{n \leq T \\ n^2 \equiv -1 \pmod{p^2}}} 1 \leq \left(1 + \left[\frac{T}{p^2}\right]\right) \sum_{\substack{x \bmod p^2 \\ x^2 \equiv -1 \pmod{p^2}}} 1 \leq 2 + \frac{2T}{p^2},$$

and so

$$A(T) \geq T - 2\sum_{p \leq T} 1 - 2T \sum_{3 \leq p \leq T} \frac{1}{p^2} = \left(1 - 2\sum_{p \geq 3} \frac{1}{p^2}\right) T + o(T).$$

Further,

$$\sum_{p \geq 3} \frac{1}{p^2} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} - 1 - \frac{1}{4} = \frac{\pi^2}{6} - \frac{5}{4} \leq \frac{5}{12},$$

and so finally

$$A(T) \geq \frac{T}{6} + o(T),$$

proving the lemma. □

Now let $D = n^2 + 1$ be square-free and consider the field $K = \mathbb{Q}(\sqrt{D})$. Its discriminant d equals either D or $4D$. The number $\eta = n + \sqrt{n^2+1} > 1$ is a unit in K, and so if $\epsilon > 1$ is a fundamental unit of K, then $\eta = \epsilon^N$ holds with some $N \geq 1$. It follows that

$$\log \epsilon = \frac{\log \eta}{N} \leq \log \eta = O(\log n) = O(\log d),$$

and this suffices to our purpose. □

The presented argument implies that there are only finitely many square-free numbers $D = n^2+1$ such that the field $\mathbb{Q}(\sqrt{D})$ has a given class-number.

4. Not much is known about the structure of $H(K)$, or $H^*(K)$, in the general case. We prove now an old result, going back to Gauss [01], which determines the number of even invariants of $H^*(K)$ for quadratic fields K.

Let K be a quadratic field, The factor-group $\mathfrak{G}(K) = H^*(K)/H^*(K)^2$ is called the *genus group* of K, and cosets mod $H^*(K)^2$ in $H^*(K)$ are called the *genera*. Denote by $g(K)$ the cardinality of $\mathfrak{G}(K)$. Obviously all non-unit elements of $\mathfrak{G}(K)$ are of order 2, thus $g(K)$ is a power of 2. The structure of $\mathfrak{G}(K)$ is determined by the following theorem:

Theorem 8.23. *If K is a quadratic number field, and t is the number of distinct prime divisors of the discriminant $d = d(K)$, then the group $\mathfrak{G}(K)$ is the product of $t-1$ copies of the group C_2.*

Proof: Write $K = \mathbb{Q}(\sqrt{D})$ with square-free D. We may assume $D \neq -1, -3$, as in these cases the theorem is trivially true.

Observe first that $\mathfrak{G}(K)$ is the maximal homomorphical image of $H^*(K)$ having the form C_2^N. Therefore it is isomorphic with the maximal subgroup V of $H^*(K)$ of that form. Obviously V coincides with the set of elements of $H^*(K)$ having their orders bounded by 2. Observe also that V can be considered as a linear space over $\mathbb{F}_2$, and we have thus to show that $\dim_{\mathbb{F}_2} V = t-1$.

Let $p_1, \ldots, p_t$ be the primes ramified in K. By Theorem 4.39 there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ such that $p_i R_K = \mathfrak{p}_i^2$ holds for $i = 1, 2, \ldots, t$. If $X_i \in H^*(K)$ is the class containing $\mathfrak{p}_i$, then $X_i^2 = E$, the unit class, thus $X_i \in V$.

We show first that if $X \neq E$, $X \in V$, then there exists an ideal $I \in X$ which is equal to its conjugate I'. To obtain this choose an unramified prime ideal $\mathfrak{p} \in X$. Its norm $N(\mathfrak{p}) = p$ is a rational prime, and we have $\mathfrak{p}\mathfrak{p}' = pR_K \in E$, implying $X' = X^{-1} = X$. Therefore $\mathfrak{p}'$ lies in X, and with a suitable totally positive $\alpha \in K^*$ we have $\mathfrak{p}' = \alpha\mathfrak{p}$. Because $N_{K/\mathbb{Q}}(\alpha)$ is positive, we get, in view of

$$p = N(\mathfrak{p}') = N_{K/\mathbb{Q}}(\alpha) N(\mathfrak{p}) = N_{K/\mathbb{Q}}(\alpha) p,$$

the equality $N_{K/\mathbb{Q}}(\alpha) = 1$. This implies $\alpha = (1+\alpha)/(1+\alpha')$ and we get

$$(1+\alpha')\mathfrak{p}' = (1+\alpha)\mathfrak{p},$$

showing that the ideal $I = (1+\alpha)\mathfrak{p} \in X$ is equal to its conjugate.

Let $m > 0$ the maximal rational integer satisfying $mR_K | I$, and write $I = mJ$. Then $J \in X$, $J' = J$ and J is not divisible by a proper ideal of the form nR_K with $n \in \mathbb{Z}$. We shall now show that J has the form

$$J = \prod_{i=1}^{t} \mathfrak{p}_i^{b_i},$$

with $b_i \in \{0, 1\}$. To do that write

$$J = \prod_{i=1}^{k} \mathfrak{P}_i^{c_i},$$

with positive exponents c_i, and observe that none of the $\mathfrak{P}_i$'s can be of degree 2, as in that case we would have $\mathfrak{P}_i = qR_K$, with a rational prime q, hence $qR_K | J$, contradiction. So all $\mathfrak{P}_i$'s are of degree one, and if one of them, say $\mathfrak{P}_1$ would be unramified, then the equality $J' = J$ would force the equality $\mathfrak{P}_1' = \mathfrak{P}_j$ with a suitable $j \neq 1$, hence $N(\mathfrak{P}_1)R_K = \mathfrak{P}_1\mathfrak{P}_1'$ would divide J, again a contradiction. We see thus that all prime ideal factors of J are ramified, and this implies that X lies in the subgroup V_0 of $H^*(K)$, generated by the classes $X_1, \ldots, X_t$. Therefore $V = V_0$, and it remains to prove that the minimal number s of generators of V_0 equals $t-1$.

Now we shall prove the inequality $s \leq t-1$, and start with the imaginary case, which is easier, as every element of K is totally positive.

If $D \not\equiv 3 \pmod 4$, then $D = -\prod_{i=1}^{t} p_i$, implying $\sqrt{D}R_K = \prod_{i=1}^{t} \mathfrak{p}_i$, and $\prod_{i=1}^{t} X_i = E$, leading to $s \leq t-1$ in this case. If, however, $D \equiv 3 \pmod 4$, then $d(K) = 4D$, hence 2 is ramified, so let $p_t = 2$. Then $D = -\prod_{i=1}^{t-1} p_i$, hence $\sqrt{D}R_K = \prod_{i=1}^{t-1} \mathfrak{p}_i$, and $\prod_{i=1}^{t-1} X_i = E$, giving again $s \leq t-1$.

If K is real, then let $\epsilon > 1$ be its fundamental unit. If $N_{K/\mathbb{Q}}(\epsilon) = -1$, then $\epsilon\sqrt{D}$ is totally positive, and the ideal generated by it is a product of some $\mathfrak{p}_i$'s. This leads to a non-trivial relation. If the norm of ϵ is positive, then write $\epsilon = a + b\sqrt{D}$ with rational and positive a, b, and observe that $\gamma = 1 + \epsilon > 0$ has positive norm, hence is totally positive. In view of

$$\gamma' = 1 + \epsilon' = 1 + 1/\epsilon = \gamma/\epsilon$$

we see that the ideal γR_K is equal to its conjugate. Therefore we can write

$$\gamma R_K = \prod_{i=1}^{t} \mathfrak{p}_i^{c_i},$$

with certain nonnegative c_i's. If all c_i's would be even, then we could write $\gamma = m\epsilon^k$ with suitable $m \in \mathbb{Z}$ and $k \geq 1$. This would imply

$$\epsilon = \frac{\gamma}{\gamma'} = \epsilon^{2k},$$

hence ϵ would be a root of unity, which is absurd. Therefore at least one c_i is odd, and this implies a non-trivial relation between the generators of V_1. Thus also in the real case we get $\dim V_1 \leq t-1$.

It remains to show that there are no other non-trivial multiplicative relations between the classes $X_1, \ldots, X_t$. Assume thus that with some $r \leq t-1$ we have $\prod_{j=1}^{r} X_{i_j} = E$. Then the product $\prod_{j=1}^{r} \mathfrak{p}_{i_j}$ is principal, generated by some totally positive $a \in R_K$. Putting $P = p_{i_1} \cdots p_{i_r}$ we get $aa' = N_{K/\mathbb{Q}}(a) = P$ and $a^2 R_K = p_{i_1} \cdots p_{i_r} R_K$. Thus, with a suitable unit u, we have

$$a^2 = uP = uaa',$$

and therefore

$$N_{K/\mathbb{Q}}(u) = N_{K/\mathbb{Q}}(a)^2 / N_{K/\mathbb{Q}}(a) N_{K/\mathbb{Q}}(a') = 1.$$

Consider first the imaginary case. The last equality implies $a' = \pm a$. If $a' = a$, then $a \in \mathbb{Q}$, its norm is a square, and so P is a square in K, which is possible only in the case, considered above. If $a' = -a$ and $a = x + y\sqrt{d}$ with $x, y \in \mathbb{Q}$, then $x = 0$, hence $a = y\sqrt{d}$ with $2y \in \mathbb{Z}$. But this implies $4P = 4a^2 = D(2y)^2$, implying $D|P$, which is possible only if $D = P$, and this shows that our relation coincides with that found before. This establishes the theorem for imaginary quadratics.

Now let K be real, and assume first that the fundamental unit $\epsilon > 0$ of K is of negative norm. In this case $u = a^2/P$ is positive, hence we can write $u = \epsilon^{2n}$ with a suitable $n \in \mathbb{Z}$. Then

$$\left(\frac{a}{(\epsilon\sqrt{D})^n}\right)' = \frac{au^{-1}}{(\epsilon^{-1}\sqrt{D})^n} = \frac{a\epsilon^{-2n}}{(\epsilon^{-1}\sqrt{D})^n} = \frac{a}{(\epsilon\sqrt{D})^n},$$

showing that the number $a/(\epsilon\sqrt{D})^n$ is invariant under the Galois group, hence rational. Thus $a = w(\epsilon\sqrt{D})^n$ holds with some $w \in \mathbb{Q}$, and we obtain

$$P = p_{i_1} \cdots p_{i_r} = N_{K/\mathbb{Q}}(a) = w^2(-1)^n(-D)^n = w^2 D^n,$$

and so n must be odd, and we obtain that P differs from D by a factor which is a rational square. This, however, is possible only in the case considered above.

Finally, let the fundamental unit $\epsilon > 0$ be of positive norm. In this case again $u > 0$, so we may write $u = \epsilon^n$ with a suitable $n \in \mathbb{Z}$. Then

$$\left(\frac{a}{(1+\epsilon)^n}\right)' = \frac{au^{-1}}{(1+\epsilon^{-1})^n} = \frac{a\epsilon^{-n}}{(1+\epsilon^{-1})^n} = \frac{a}{(1+\epsilon)^n},$$

thus the number $w = a/(1+\epsilon)^n$ is rational. Therefore $P = w^2(N_{K/\mathbb{Q}}(1+\epsilon))^n$, and we see that n is odd, as otherwise P would be a square. Now let $P_1 = p_1 \cdots p_t/P$, and consider the ideal

$$I = \prod_{\substack{1 \le i \le t \\ i \ne i_1, \ldots, i_r}} \mathfrak{p}_i = (\sqrt{P_1})R_K.$$

Repeating our argument with P_1 in place of a we get

$$P_1 = w_1^2(N_{K/\mathbb{Q}}(1+\epsilon))^m,$$

with rational w_1 and odd m. This implies

$$p_1 \cdots p_t = PP_1 = (ww_1)^2(N_{K/\mathbb{Q}}(1+\epsilon))^{m+n},$$

but the right-hand side is a square, whereas on the left-hand side we have a square-free integer $\neq 1$, contradiction. □

Corollary 1. *If $K/\mathbb{Q}$ is quadratic, then the group $H^*(K)$ has $\omega(d) - 1$ even invariants, $\omega(N)$ being the number of distinct prime divisors of an rational integer N.*

Proof : If $H^*(K) = \prod_i C_{n_1}$ is the factorization of $H^*(K)$ with cyclic factors, then the canonical map of $H^*(K)$ onto $\mathfrak{G}(K)$ trivializes every factor with n_i odd, whereas every factor with n_i even becomes a non-trivial cyclic factor of $\mathfrak{G}(K)$. Thus the number of even n_i's equals the number of non-trivial cyclic factors of $\mathfrak{G}(K)$, because for even n_i, n_j, with $i \ne j$, the images of C_{n_i} and C_{n_j} cannot coincide. □

Corollary 2. *The narrow class-number $h^*(K)$ of a quadratic number field K is odd if and only if the discriminant of K is a prime-power, i.e., $d = -4$, ± 8, $(-1)^{(p-1)/2}p$ (with odd prime p.*

Proof : A trivial deduction from the preceding corollary. □

As an application of the theorem just proved we present now a quadratic field whose class-group $H(K)$ is a direct factor of $H^*(K)$, and also a field in which this does not hold.

First let $K = \mathbb{Q}(\sqrt{34})$. Here $d(K) = 2^3 \cdot 17$, $\omega(d(K)) = 2$, hence $H^*(K)$ has one even invariant. The fundamental unit has positive norm, because the unit $35 + 6\sqrt{34}$ has positive norm, but it is not a square in K, and by Corollary 2 to Theorem 3.25 one gets $h^*(K) = 2h(K)$. By Lemma 3.8 in every ideal class of $H(K)$ there is an ideal with norm not exceeding 5, and a routine examination of the ideals involved leads us to $h(K) = 2$, whence $H(K) = C_2$. Since $h^*(K) = 2h(K) = 4$ we obtain $H^*(K) = C_4$, and so $H(K)$ is not a direct factor of $H^*(K)$.

Now let $K = \mathbb{Q}(\sqrt{15})$. Here $d(K) = 2^2 \cdot 3 \cdot 5$, $\omega(d(K)) = 3$. The norm of the fundamental unit is positive, since the equation $x^2 - 15y^2 = -1$ has no solutions, even mod 3. Consequently $h^*(K) = 2h(K)$ and the inspection of ideals with small norms gives $h(K) = 2$, thus $H^*(K) = C_2 \times C_2$, and we see that in this case $H(K)$ is a direct factor of $H^*(K)$.

We conclude this subsection with an asymptotic result concerning the number $g(d)$ of genera for negative d.

Proposition 8.24. *If d tends to $-\infty$ then the quotient $g(d)/h(d)$ tends to zero.*

Proof : Assume that for an infinite sequence d_k of negative quadratic discriminants we have $h(d_k) \leq Bg(d_k)$ with some fixed B. Corollary 1 to Theorem 8.14 implies $g(d_k) \to \infty$, and so by Theorem 8.23 the number $t_k = \omega(d_k)$ tends to infinity with k. Observe now that if p_{t_k} is the t_k-th consecutive prime, then

$$\log |d_k| \geq \sum_{p|d_k} \log p \geq \sum_{p \leq p_{t_k}} \log p,$$

and by an elementary result of Chebyshev the last sum exceeds $C_1 p_{t_k} \geq C_2 t_k \log t_k$ for some positive C_1, C_2. Using again Corollary 1 to Theorem 8.14 we get for large k the inequality

$$h(d_k) \geq |d_k|^{1/4} \geq \exp(C_3 t_k \log t_k)$$

with a suitable $C_3 > 0$, and so finally we arrive at

$$\exp(C_3 t_k \log t_k) \ll g(d_k) = 2^{t_k - 1} = \exp((t_k - 1)\log 2),$$

which is a clear contradiction for t_k large enough. □

Corollary. *For sufficiently large N there is no imaginary quadratic field whose class group is the product of N copies of C_2.*

Proof : If $H(K) = C_2^N$, then $H(K) = H^*(K) = \mathfrak{G}(K)$, hence $g(K) = h(K)$, and the proposition implies that this can hold only for finitely many imaginary quadratic fields. □

5. It follows from Theorem 8.23 that for any power of 2 there exist infinitely many quadratic fields with class-number divisible by it. We present now a result of Nagell [22] which asserts that the same holds for any positive integer, if we restrict attention to imaginary quadratic fields.

Theorem 8.25. *If n is an arbitrary positive rational integer, then there exist infinitely many imaginary quadratic fields with class-number divisible by n.*

The proof of this theorem will be based on the following auxiliary result:

Lemma 8.26. *Let $D > 3$ be a square-free rational integer, and $q = p^a$ a prime power, p being an odd prime. Assume that the equation*

$$x^2 + Dy^2 = z^q$$

has a solution x, y, z with $(x, y) = 1$, $2 \nmid z$, $p|x$ and $p^2 \nmid x$. Then for the field $K = \mathbb{Q}(\sqrt{-D})$ we have $q|h(K)$.

Proof : Our equation may be written in the form

$$JJ' = N(J)R_K = z^q R_K,$$

where J is the principal ideal generated by $\xi = x + y\sqrt{-D}$, and J' is its conjugate. Our assumptions imply $(J, J') = 1$, hence J must be a q-th power of an integral ideal, say $J = I^q$. Assume, contrary to our assertion, that $p^b \parallel h(K)$ and $b < a$. Then $(q, h(K)) = p^b$, and with suitable $A, B \in \mathbb{Z}$ we obtain

$$Aq + Bh(K) = p^b,$$

showing that the ideal $I^{p^b} = J^A I^{Bh(K)}$ is principal. Now J is a p-th power of a principal ideal, and since the only units in K are ± 1, it follows that ξ is a p-th power of an integer in K. We have now to distinguish between two cases:

(a) $D \equiv 1$ or $2 \pmod 4$,
and
(b) $D \equiv 3 \pmod 4$.

In the case (a) we can write

$$x + y\sqrt{-D} = \xi = (u + v\sqrt{-D})^p$$

with suitable $u, v \in \mathbb{Z}$, which are relatively prime in view of $(x, y) = 1$. Comparing the rational parts on both sides of this equality we get

$$x = u^p - \binom{p}{2} u^{p-2}v^2 D + \cdots + \binom{p}{p-1} uv^{p-1}(-D)^{(p-1)/2},$$

thus

$$0 \equiv x \equiv u \pmod p,$$

and this shows $p^2|u^p$, thus $p^2|x$, giving a contradiction.

In the case (b) we proceed in a similar way. Write

$$x + y\sqrt{-D} = \xi = \left(u + \frac{v}{2} + \frac{v}{2}\sqrt{-D}\right)^p$$

with suitable relatively prime rational integers u, v. Putting $t = 2u + v$ and proceeding as in the previous case we get

$$2^p x = t^p - \binom{p}{2} t^{p-2}v^2 D + \cdots + \binom{p}{p-1} tv^{p-1}(-D)^{(p-1)/2},$$

and from $p|x$ we infer $p|t$. Hence $p^2|2^p x$ and $p^2|x$, which is a contradiction. □

Corollary. *Let $D > 3$ be a square-free rational integer, and let n be an odd integer. Assume that the equation*

$$x^2 + Dy^2 = z^n$$

has a solution x, y, z with $(x, y) = 1$, $2 \nmid z$ and (x, n^2) equal to n^*, the product of all distinct primes dividing n. Then the class-number $h(K)$ of the field $K = \mathbb{Q}(\sqrt{-D})$ is divisible by n.

Proof : Immediate from the lemma. □

Proof of the theorem: Let m be a given odd number, and let x be an integer satisfying $(m, x) = m^*$. Then the polynomial $X^m - x^2$ is irreducible over $\mathbb{Q}$, because x^2 is not a m_1-th power for any non-trivial divisor m_1 of m. As we already have seen in the proof of Theorem 4.37 this implies that the congruence $z^m \equiv x^2 \pmod{p}$ has solutions in z for infinitely many primes p. We can even obtain solutions with $z^m \equiv x^2 \pmod{p^2}$, replacing z, if necessary, by $z + p$. By the Chinese remainder theorem we can now obtain, for any r, infinitely many sets $A = \{p_1, \ldots, p_r\}$ of r primes such that with some $z_A \in \mathbb{Z}$ we have $p_i \parallel z_A^m - x^2 > 0$ $(i = 1, 2, \ldots, r)$ and $p_i \nmid z_A x$. Write $z_A^m - x^2 = D_A y_A^2$ with square-free D_A. Since the product $p_1 \cdots p_r$ divides D_A, hence by Theorem 8.23 the class-number of $K_A = \mathbb{Q}(\sqrt{-D_A})$ is divisible by 2^{r-1}.

To apply the corollary to the last lemma observe that we can always choose z_A to be odd (replacing z_A, if necessary, by $z_A + (p_1 \cdots p_r)^2$), and, moreover, that the condition $(x, y_A) = 1$ is also fulfilled. Indeed, if q is a prime divisor of (x, y_A) and $q \notin A$, then replacing z_A by $z_A + u(p_1 \cdots p_r)^2$ with a suitable $u \in \mathbb{Z}$, we can obtain $(z_A, q) = 1$. If $a \in A$, then we have $(z_A, q) = 1$ by construction, and it remains to observe that $q|(x, y_A)$ implies $q|z_A$.

Thus we may apply the last corollary to get the divisibility of $h(K)$ by m. We have obtained thus infinitely many imaginary quadratic fields with class-number divisible by $2^{r-1}m$, where $r \geq 1$ is arbitrary and m is an arbitrary odd positive integer. This establishes the theorem. □

6. Theorem 8.23 implies that if a quadratic field has sufficiently many ramified primes, then its class-number is larger than any prescribed positive number. An analogue of this result for arbitrary normal extensions of a fixed degree will be deduced from the following theorem giving a sufficient condition for the existence of large subgroups in $H(K)$:

Theorem 8.27. *There exists a function $c(n)$ with the following properties: for any prime q and any field K of degree n the class-group $H(K)$ contains C_q^N as a subgroup, with*

$$N \geq t_q - c(n),$$

where $t_q = t_q(K)$ *denotes the number of rational primes* p *such that the ramification indices of all prime ideals of* R_K *lying over* $p\mathbb{Z}$ *are divisible by* q.

Moreover, if $q \neq 2$, $r(K)$ *is the unit rank of* K, $\overline{K}$ *is the field complex conjugated to* K, *and for any field* L *we denote by* $A_q(L)$ *the degree of the composite of all pure fields* $\mathbb{Q}(a^{1/q})$ *(with* $a \in \mathbb{Q}$*) contained in* L, *then*

$$N \geq t_q - c_1(K),$$

where

$$c_1(K) = \begin{cases} r(K) + \log A_q(K)/\log q & \text{if } \zeta_q \in K, \\ r(K) + \log A_q((K\overline{K})^+)/\log q & \text{if } \zeta_q \notin K. \end{cases}$$

Proof : Let C_q^N be the maximal subgroup of the form C_q^T of $H(K)$. It equals H_q/H_q^q, where H_q is the q-Sylow subgroup of $H(K)$. Denote by I_q the group of all non-zero elements of K which generate q-th powers of fractional ideals, and put $P = (K^*)^q$, $U = U(K)$ and $E = E(K)$. Then $H_q/H_q^q \sim I_q/UP$ and the sequence

$$1 \longrightarrow UP/EP \longrightarrow I_q/EP \longrightarrow I_q/UP \longrightarrow 1$$

is exact. Since all its terms can be regarded as vector spaces over $k = \mathbb{F}_q$ we get

$$N = \dim_k I_q/UP = \dim_k I_q/EP - \dim_k UP/EP.$$

Theorem 3.13 gives

$$\dim_k UP/EP = \dim_k U/EU^q = r(K),$$

and so it remains to obtain a good lower bound for $\dim_k I_q/EP$. Let $t = t_q$ and let $p_1, \ldots, p_t$ be rational primes, whose all prime ideals divisors in K have their ramification indices divisible by q. All these primes lie in I_q, so let X be the subspace of I_q/EP generated by their images. If $s = \dim_k X$, then there are $M = t - s$ independent linear relations between our generators of X. This shows that with suitable $0 \leq x_{ij} \leq q-1$, $A_j \in K^*$ and $z_j \in E$ $(i = 1, 2, \ldots, t; j = 1, 2, \ldots, M)$ we have

$$b_j = \prod_{i=1}^{t} p_i^{x_{ij}} = z_j A_j^q \quad (j = 1, 2, \ldots, M), \tag{8.15}$$

and $\operatorname{rank}_k[x_{ij}] = M$.

Observe that for any positive integer c and $M \geq M(c, n)$ at least $c+1$ numbers z_j are equal, say $z_1 = z_2 = \ldots = z_{c+1}$, thus $b_j/b_{1+c} = B_j^q$ holds for $j = 1, 2, \ldots, c$ with suitable $B_j \in K$. Hence for $j = 1, 2, \ldots, c$ the field K contains the field generated by $(b_j b_{c+1}^{q-1})^{1/q}$. Observe further that the numbers

$b_j b_{c+1}^{q-1}$ are q-independent in $\mathbb{Q}$. Indeed, otherwise we would have with suitable $0 \le y_1, \dots, y_c < q$, not all vanishing, and an $r \in \mathbb{Z}$, the equality

$$\prod_{j=1}^{c} (b_j b_{c+1}^{q-1})^{y_j} = r^q.$$

Thus

$$\prod_{i=1}^{t} p_i^{a_i} = r^q,$$

where

$$a_i = \sum_{j=1}^{c} y_j (x_{ij} + x_{i,c+1}(q-1)).$$

However

$$0 \equiv a_i \equiv \sum_{j=1}^{c} y_j (x_{ij} - x_{i,c+1}) \pmod{q},$$

and since $\operatorname{rank}_k [x_{ij} - x_{i,c+1}] = c$, all y_j's must vanish.

Lemma 7.41 (iii) implies now $q^c | n$, thus $c \le \log n / \log q$, hence M must be bounded. In view of the equality $N = t - M - r(K) = t + O(1)$ this gives the first assertion.

If q is odd, then one obtains a better upper bound for M proceeding as follows: take the complex conjugate of both sides of (8.15), and multiply pairwise. This leads to $b_j^2 = B_j^q$ with $B_j = A_j \overline{A}_j \in (K\overline{K})^+$ for $j = 1, 2, \dots, M$. Since the b_j's are q-independent in $\mathbb{Q}$ and $q \neq 2$, so are the b_j^2's. Consequently the field $(K\overline{K})^+$ contains the composite of all fields $\mathbb{Q}((b_j^2)^{1/q})$ which is of degree q^M, thus $q^M \le A_q((K\overline{K})^+)$. If K does not contain ζ_q, all b_j's are q-th powers in K, and the same argument leads to $q^M \le A_q(K)$. This establishes the last assertion, and we see that one can have $c(n) = \max\{c_1(K) : [K : \mathbb{Q}] = n\}$. □

Corollary 1. *If p is an odd prime and $K/\mathbb{Q}$ is a pure extension of degree p, then $H(K)$ has at least $t_p - p$ invariants divisible by p.*

Proof : Here $A_p(K) = p$ and $\zeta_p \notin K$, thus $c_1(K) = r(K) + 1 = p$. □

Corollary 2. *If $K/\mathbb{Q}$ is either Abelian or totally real, and p is an odd prime, then $H(K)$ has at least $t_p - r(K)$ invariants divisible by p.*

Proof : In this case $A_p(K) = A_p((KK^+)) = 1$. □

Note that this corollary fails to hold for $p = 2$ in the case of imaginary quadratic fields, as shown in Theorem 8.23.

Corollary 3. *If $K/\mathbb{Q}$ is cyclic of an odd prime degree p, then $H(K)$ has at least $\omega(d(K)) - p + 1$ invariants divisible by p.*

Proof : In this case every ramified prime is counted by t_p, thus $t_p = \omega(d(K))$ and since $r(K) = p-1$ the assertion follows from the preceding corollary. □

Corollary 4. *If $K_1, K_2, \ldots$ is a sequence of normal extensions of $\mathbb{Q}$ of a fixed degree n and $\omega(d(K_j))$ tends to infinity, then $\lim_j h(K_j) = \infty$.*

Proof : Since every prime ramified in $K_i/\mathbb{Q}$ is counted by $t_p(K_i)$ for a certain prime divisor p of n, the number

$$\max\{t_p(K_i) : \ p|n\}$$

tends to infinity, and we may apply the theorem. □

7. Finally we turn to imaginary quadratic fields with class-number one, and start with a curious result of Frobenius [12] and Rabinowitsch [13], displaying a connection between these fields and the problem of representing primes by quadratic polynomials.

Theorem 8.28. *Let K be an imaginary quadratic field with discriminant $d \neq -3, -4, -8$. Then $h(K) = 1$ holds if and only if $d \equiv 1 \pmod 4$, and for $x = 1, 2, \ldots, (1-d)/4 - 1$ the polynomial*

$$F_d(X) = X^2 - X + \frac{1-d}{4}$$

attains exclusively prime values.

Proof : Let K be an imaginary quadratic field with $h(K) = 1$ and $d = d(K) \neq -3, -4, -8$. Observe first that Corollary 2 to Theorem 8.23 implies that $d \equiv 1 \pmod 4$. Put $\omega = (1+\sqrt{d})/2$, and recall that $1, \omega$ is an integral basis for K. For $x \in \mathbb{Z}$ we have $N_{K/\mathbb{Q}}(x+\omega) = F_d(x)$, and for $x = 1, 2, \ldots, (1-d)/4$ the inequality $N_{K/\mathbb{Q}}(x+\omega) < (1-d)^2/16$ holds. Note that for x in this range the numbers $x+\omega$ are all irreducible, independently of the assumption $h(K) = 1$. Indeed, from $x + \omega = ab$ we infer $N_{K/\mathbb{Q}}(ab) < (1-d)^2/16$, and so the norm of one of the factors, say of b, does not exceed $(1-d)/4$. But if $r + s\omega$ is an arbitrary irrational element of R_K (i.e., $s \neq 0$), then

$$N_{K/\mathbb{Q}}(r+sw) = r^2 - rs + (1-d)s^2/4 = (r - s/2)^2 + |d|s^2/4,$$

and this exceeds $(1-d)/4$. Thus b must be rational and it suffices to observe that $x + \omega$ does not have rational integral divisors except ± 1, and so is irreducible.

Now we use the assumption $h(K) = 1$ to infer that the elements $x + \omega$ generate prime ideals, and so their norms are either primes or squares of

primes. The last possibility could arise only if $x+\omega$ happened to be rational, which is impossible, and so the values of $F_d(x) = N_{K/\mathbb{Q}}(x+\omega)$ are rational primes for $x = 1, 2, \ldots, (1-d/4)-1$, proving the necessity of the condition stated.

To prove its sufficiency assume that $d \equiv 1 \pmod 4$ (thus $|d| > 7$), and that for $x = 1, 2, \ldots, (1-d/4)-1$ the numbers $F_d(x)$ are prime. Assume moreover $h(K) > 1$, and choose a non-principal ideal I with the least norm. Obviously it must be a prime ideal and its norm has to be a rational prime, say p, not exceeding $2\sqrt{|d|}/\pi$, in view of Lemma 3.8.

As the index of $\omega = (1+\sqrt{d})/2$ equals 1, and $F_d(X)$ is its minimal polynomial, Theorem 4.33 shows that

$$pR_K = IJ, \quad I = pR_K + (\omega - \omega_1)R_K, J = pR_K + (\omega - \omega_2)R_K,$$

where ω_1, ω_2 are solutions of the congruence $F_d(x) \equiv 0 \pmod p$. We may assume that $1 \leq \omega_i \leq p-1$ holds for $i = 1, 2$. Let $\xi = w + p - w_1$. The norm N of ξ equals $F_d(p-\omega_1)$, and since

$$0 < p - \omega_1 \leq p - 1 \leq 2\sqrt{|d|}/\pi < (1-d)/4$$

holds for $|d| \geq 7$, our assumption implies that N is a prime. Now observe that ξ lies in I, and therefore

$$N_{K/\mathbb{Q}}(\xi) = N = p = N(I),$$

leading to $\xi R_K = I$, and so I is principal, a contradiction. □

8. We conclude this section with an upper bound for the absolute value of the discriminant of an imaginary quadratic field with class-number one. We follow Bundschuh and Hock [69], but use a stronger version of Baker's method.

Theorem 8.29. *If K is an imaginary quadratic field with $h(K) = 1$, then $|d(K)| \leq 6 \cdot 10^{56}$.*

Proof : According to Corollary 2 to Theorem 8.23, if $|d(K)| \geq 10$ and $h(K) = 1$, then $d(K) = -p$, where $p \equiv 3 \pmod 4$ is a prime. We show now that p must be congruent to 3 mod 8.

Lemma 8.30. *If $d = d(K) = -p < -10$ and $h(K) = 1$, then p is congruent to 3 (mod 8).*

Proof : Assume to the contrary that $p \equiv 7 \pmod 8$. Since $(p+1)/4 > 2$ is even we can write $(p+1)/4 = 2a$ with $a \geq 2$. Consider the quadratic form $2X^2 + XY + aY^2$, which is of discriminant d. In view of $h(K) = 1$ this form must be, according to Theorem 8.18, equivalent to every positive definite and primitive form of discriminant d, and so, in particular, it must be equivalent to the form $X^2 + 2aY^2$. Since the latter represents 1, the same must be true

for f. This is not possible, because for $x \in \mathbb{Z}$ we have $f(x,0) = 2x^2 \neq 1$, and if y is a non-zero rational integer, then for $x \in \mathbb{Z}$ we have

$$f(x,y) = 2\left(x + \frac{y}{4}\right)^2 + \frac{py^2}{8} \geq \frac{p}{8} > 1. \qquad \square$$

The next lemma provides an analytic identity on which the proof of the theorem rests. We use the following notation: $Q(X,Y)$ is the quadratic form $X^2 + XY + \frac{1}{4}(p-1)Y^2$ of discriminant d, χ is the primitive character induced by the unique non-principal character in $X(K)$, and for prime $q \neq 2$ we denote by χ_q the unique primitive real character mod$q$. In what follows we assume that $|d|$ exceeds 200.

Lemma 8.31. *If $q \equiv 1 \pmod 4$ is a prime, then for* Re $s > 1$ *the following identity holds:*

$$L(s,\chi_q)L(s,\chi\chi_q) = \zeta(2s)\left(1 - \frac{1}{q^{2s}}\right)$$
$$+ \frac{1}{q}\left(\frac{p}{4}\right)^{1/2-s} \sqrt{\pi}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}(q^{2-2s}-1)\zeta(2s-1) + R_q(s), \qquad (8.16)$$

where

$$R_q(s) = \frac{1}{q}\left(\frac{p}{4}\right)^{1/2-s} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{q-1} \chi_q(Q(m,y)) \sum_{k\neq 0} T_k(m,y,s),$$

$$T_k(m,y,s) = \exp\left(\frac{2\pi ik(m+y/2)}{q}\right) J_2(ky,s)$$

and

$$J_2(N,s) = \int_{-\infty}^{\infty} \frac{\exp(-\pi i N\sqrt{p}u/q)}{(1+u^2)^s} du.$$

Proof : We start with the identity

$$L(s,\chi_q)L(s,\chi\chi_q) = \sum_{m,n=1}^{\infty} \frac{\chi_q(mn)\chi(m)}{(mn)^s}$$
$$= \sum_{r=1}^{\infty} \frac{\chi_q(r)}{r^s} \sum_{d|r} \chi(d),$$

valid for Re $s > 1$.

Comparing the coefficients of the Dirichlet series on both sides of the equality $\zeta_K(s) = \zeta(s)L(s,\chi)$, resulting from Theorem 8.6, we see that

$$F(r) = \sum_{d|r} \chi(d)$$

equals the number of ideals of R_K with norm r. Now every ideal of R_K is principal, and since K contains only two roots of unity, $F(r)$ equals $G(r)/2$, where $G(r)$ denotes the number of integers of R_K with norm r. Since an integral basis of K is formed by 1 and $\omega = (1+\sqrt{d})/2$, and $N_{K/\mathbb{Q}}(x+y\omega) = Q(x,y)$, we obtain finally that $2F(r)$ equals the number of representations of an integer r by the form Q (This is the only point of the proof where we use the assumption $h(K) = 1$.)

It follows that

$$L(s,\chi_q)L(s,\chi\chi_q) = \frac{1}{2}\sum_{x\neq 0} \frac{\chi_q(Q(x,0)}{Q(x,0)^s} + \frac{1}{2}\sum_{y\neq 0} \frac{\chi_q(Q(x,y))}{Q(x,y)^s}.$$

The first summand equals

$$\frac{1}{2}\sum_{x\neq 0} \frac{\chi_q(x^2)}{x^{2s}} = \sum_{\substack{x\geq 1\\ q\nmid x}} \frac{1}{x^{2s}} = \zeta(2s)\left(1-\frac{1}{q^{2s}}\right),$$

hence it agrees with the first summand in (8.16).

The second summand is more complicated, and requires some stronger tools. Let us call this summand S and using the equality $Q(-x,-y) = Q(x,y)$, write S in the form

$$\begin{aligned} S &= \sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty} \frac{\chi_q(Q(x,y))}{Q(x,y)^s} \\ &= \sum_{y=1}^{\infty}\sum_{m=0}^{q-1} \chi_q(Q(m,y)) \sum_{x=-\infty}^{\infty} \frac{1}{Q(qx+m,y)^s}. \end{aligned}$$

Now we apply Poisson's formula (Theorem VIII of Appendix I) for $G = \mathbb{R}^+$ and $H = \mathbb{Z}$ to get

$$S = \sum_{y=1}^{\infty}\sum_{m=0}^{q-1} \chi_q(Q(m,y)) \sum_{k=-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{\exp(-2\pi ikt)}{Q(qt+m,y)^s} dt.$$

Making the substitution $m + qt + y/2 = yu\sqrt{p}/2$ in the inner integral, and noting that $Q(x,y) = (x+y/2)^2 + py^2/4$ we obtain

$$S = \frac{1}{q}\left(\frac{p}{4}\right)^{1/2-s} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{q-1} \chi_q(Q(m,y))G(m,y),$$

where

$$G(m,y) = \sum_{k=-\infty}^{\infty} \exp\left(\frac{2\pi ik}{q}\left(m+\frac{y}{2}\right)\right) J_2(ky,s).$$

In the last equality put $z = ky$, and isolate the term corresponding to $z = 0$, which equals

$$\begin{aligned} S_0 &= \frac{1}{q}\left(\frac{p}{4}\right)^{1/2-s} \int_{-\infty}^{\infty} \frac{du}{(1+u^2)^s} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{q-1} \chi_q(Q(m,y)) \\ &= \frac{1}{q}\left(\frac{p}{4}\right)^{1/2-s} \sqrt{\pi}\frac{\Gamma(s-1/2)}{\Gamma(s)} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{q-1} \chi_q(Q(m,y)). \end{aligned}$$

Since $q \equiv 1 \pmod 4$, the character χ_q is even, and Proposition 6.14 (i) and Theorem 6.16 imply

$$\chi_q(a) = \frac{\tau_1(\chi_q)}{\tau(\chi_q)} = \frac{\tau_a(\chi_q)}{\sqrt{q}}.$$

Thus

$$\sum_{m=0}^{q-1} \chi_q(Q(m,y)) = \frac{1}{\sqrt{q}} \sum_{j=1}^{q-1} \chi_q(j) \sum_{m=0}^{q-1} \exp(2\pi i j Q(m,y)/q).$$

Put $M = (q+1)/2$ and observe that

$$Q(m,y) \equiv (m+My)^2 + pM^2y^2 \pmod q,$$

and since by Proposition 6.14 (i) and Theorem 6.16 we have

$$\sum_{n=0}^{q-1} \exp(2\pi i j n^2/q) = \left(\frac{j}{q}\right)\sqrt{q} = \chi_q(j)\sqrt{q},$$

we arrive at

$$\begin{aligned} \sum_{m=0}^{q-1} \chi_q(Q(m,y)) &= \frac{1}{\sqrt{q}} \sum_{j=1}^{q-1} \chi_q(j) \exp(2\pi i j p M^2 y^2/q) \sum_{n=0}^{q-1} \exp(2\pi i j n^2/q) \\ &= \sum_{j=0}^{q-1} \exp(2\pi i j p M^2 y^2)/q) = \begin{cases} q-1 & \text{if } q|y, \\ -1 & \text{otherwise.} \end{cases} \end{aligned}$$

This gives

$$\begin{aligned} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{q-1} \chi_q(Q(m,y)) &= \sum_{\substack{y>0 \\ q|y}} (q-1)y^{1-2s} - \sum_{\substack{y>0 \\ q\nmid y}} y^{1-2s} \\ &= (q^{2-2s}-1)\zeta(2s-1), \end{aligned}$$

and we see that S_0 coincides with the second term on the right-hand side of (8.16). One realizes immediately that the remaining part of S equals $R_q(s)$ and so equality (8.16) results. □

The formula for the product of two L-functions, obtained in the last lemma, has an advantage over other possible formulas of that type, because the remainder term $R_q(s)$ is very small at $s = 1$, and this will enable us to apply Baker's method. An evaluation of $R_q(s)$ is contained in the next lemma:

Lemma 8.32. *The series defining $R_q(s)$ converges in a neighbourhood of $s = 1$ to a continuous function, and if $q \leq 13$ and $p \geq 200$, then*

$$|R_q(1)| \leq \frac{14}{\sqrt{p}} \exp(-\pi\sqrt{p}/q).$$

Proof : The first assertion follows from the estimate

$$|J_2(ky, s)| \ll (ky)^{-2}$$

holding for $k \neq 0$ in a neighbourhood of $s = 1$, which can be obtained from the definition of J_2 by iterated partial integration. To prove the second assertion we have to compute $J_2(ky, 1)$. Write

$$A = -\pi k\sqrt{p}/q \quad \text{and} \quad f(z) = \frac{\exp(iAz)}{1+z^2}.$$

Let R be a large positive number, and integrate f over the upper half of the circle $|z| = R$ if k is positive, and over the lower half of that circle if k is negative. Since these integrals tend to zero when R goes to infinity, the residue theorem leads to

$$J_2(ky, 1) = \pi\xi^{|ky|}$$

with $\xi = \exp(-\pi\sqrt{p}/q) < 1$. This yields

$$\begin{aligned} |R_q(1)| &\leq \frac{2}{q\sqrt{p}} \sum_{y\geq 1} \sum_{m=0}^{q-1} \sum_{k\neq 0} |J_2(ky, 1)| \leq \frac{2\pi}{\sqrt{p}} \sum_{y\geq 1} \sum_{k\neq 0} \xi^{|ky|} \\ &\leq \frac{4\pi}{\sqrt{p}} \sum_{y\geq 1} \sum_{k\geq 1} \xi^{|ky|} = \frac{4\pi}{\sqrt{p}} \sum_{y\geq 1} \frac{\xi^y}{1-\xi^y} \\ &\leq \frac{4\pi}{\sqrt{p}(1-\xi)} \sum_{y\geq 1} \xi^y = \frac{4\pi\xi}{\sqrt{p}(1-\xi)^2}. \end{aligned}$$

Using the inequalities $p \geq 200$ and $q \leq 13$ we get $(1-\xi)^{-2} \leq 1.07$, and our assertion follows in view of $1.07 \cdot 4\pi < 14$. □

Letting in (8.16) s tend to 1, which is allowed by the last lemma, we get

$$L(1, \chi_q)L(1, \chi\chi_q) = \frac{\pi^2}{6}\left(1 - \frac{1}{q^2}\right) + \frac{2\log q}{q\sqrt{p}} + R_q(1).$$

Putting in this equality first $q = 5$ and multiplying by $168/169$, and then putting $q = 13$ and multiplying by $24/25$ we obtain by subtraction

$$\frac{168}{169}L(1,\chi_5)L(1,\chi\chi_5)-\frac{24}{25}L(1,\chi_{13})L(1,\chi\chi_{13})+\frac{2\pi}{\sqrt{p}}\left(\frac{168}{845}\log 5-\frac{24}{325}\log 13\right)$$
$$=\frac{168}{169}R_5(1)-\frac{24}{25}R_{13}(1).$$

Proposition 8.12 shows that

$$L(1,\chi_5)=\frac{\log a}{\sqrt{5}},\quad L(1,\chi_{13})=\frac{\log b}{\sqrt{13}},$$

with $a=(1+\sqrt{5})/2$ and $b=(3+\sqrt{13})/2$, and we infer from Corollary 2 to Theorem 8.10 that

$$L(1,\chi\chi_5)=h(K_1)/\sqrt{5p},\quad L(1,\chi\chi_{13})=h(K_2)/\sqrt{13p},$$

where $K_1=\mathbb{Q}(\sqrt{-5p})$, $K_2=\mathbb{Q}(\sqrt{-13p})$ and taking $c=5^{1680}13^{-624}$ we obtain

$$840h(K_1)\log a-312h(K_2)\log b+\log c=\frac{\sqrt{p}}{\pi}(4200R_5(1)-4056R_{13}(1)).$$

Corollary to Theorem 4.10 shows that for $p>10^{11}$ we have

$$h(K_1)<\frac{4}{5}\sqrt{p}\log p\quad\text{and}\quad h(K_2)<\frac{4}{3}\sqrt{p}\log p,$$

hence, applying Lemma 8.31 we get

$$|x_1\log a+x_2\log b+\log c|\le 36\,791\exp(-\pi\sqrt{p}/5)\le\exp(11-\pi\sqrt{p/5})$$

with $x_1,x_2\in\mathbb{Z}$, $|x_i|\le 672\sqrt{p}\log p$. Denoting by $H(u)$ the height of a number u, as defined in Appendix III, we have $H(a)=1$, $H(b)=3$ and $H(c)\le\exp(2704)$. Moreover, $x_1\log a+x_2\log b+\log c$ does not vanish, since otherwise we would have $a^{x_1}b^{x_2}c=1$, implying $b^{x_2}\in\mathbb{Q}(\sqrt{5})$, which is impossible. Observe finally that the field $\mathbb{Q}(a,b,c)$ is of degree 4. Applying Baker's theorem in the form given in Appendix III with $A_1=e$, $A_2=3$, $A_3=\exp(2704)$, $C=192^{600}<\exp 3155$, $M=700\sqrt{p}\log p<p$, we get

$$\log(|x_1\log a+x_2\log b+\log c|)\ge -2971e^{52}\log p.$$

Hence

$$2971e^{52}\log p\ge\frac{\sqrt{p}}{5}-11,$$

implying $p\le\exp(130.67)<6\cdot 10^{56}$, as asserted. □

8.4. Notes to Chapter 8

1. The results presented at the beginning of this chapter are specializations of the class-field theory to the case of the rational ground field, in which case they are elementary consequences of the Kronecker-Weber theorem and Chebotarev's density theorem. Cf. Carlitz [33].

Corollary to Proposition 8.1 is essentially due to Hilbert [97] (see also Speiser [16]). An analogue of Corollary to Proposition 8.1 for infinite Abelian extension appears in Lundström [01].

It follows from Theorem 6.16 that the conductor of a quadratic field K equals $|d(K)|$. Formulas expressing the conductor of cyclic cubic, resp. quartic fields K in terms of the coefficients of the minimal polynomial of an integral generator of K were given in Huard, Spearman, Williams [94] and Spearman, Williams [96c], respectively.

An analogue of Theorem 8.6 is valid for arbitrary extensions L/K of algebraic number fields, the quotient $\zeta_L(s)/\zeta_K(s)$ being in this case the product of suitable Artin L-functions. In the Abelian case this quotient is a product of zeta-functions associated with characters of a suitable group $H_I^*(K)$. See e.g. Cassels, Fröhlich [67], Hasse [26c], Lang [70], Neukirch [92]. Ankeny [52a] asserted a kind of a converse to Theorem 8.6, stating that if $F(s)$ is a product of a finite set of Dirichlet L-functions with at most one factor corresponding to a trivial character, and the Dirichlet series of F has non-negative coefficients, then F is the Dedekind zeta-function of some Abelian extension of the rationals. For a simple proof see Iwasaki [52].

2. The formula appearing in Proposition 8.7. is known as the *conductor-discriminant formula.* An analogue of it holds for all relative Abelian extensions. See Hasse [30c], [34], Tatuzawa [73c], Vassiliou [33]. For the non-Abelian case see Artin [31].

It seems that Theorem 8.8 has never been explicitly stated, although all ingredients of its proof are contained in the paper of Kubota [56a], on which our approach is modelled. Lemma 8.9 is due to Delsarte [48], and the proof given by us is that of Wiegandt [59]. A more precise version of Theorem 8.8 has been obtained by Mäki [88], [93].

It was shown in Sarbasov [67] that in Corollary 2 to Theorem 8.8 in case of $p \geq 5$ the remainder term is $O(x^a)$ for every $a > 1/(p-1) - 3/(p+3)$. For $p = 3$ one can take here any $a > 1/4$ (Urazbaev [54]). Asymptotics for the number of extensions of $\mathbb{Q}$ with Galois group C_p^N and bounded discriminant was determined by Zhang X. [84b,c]. Its main term can be also obtained from Corollary 1 to Theorem 8.8. For octic fields with Galois group C_2^3 see Baily [81] Several papers by Urazbaev and his collaborators dealt with analogous problems for various classes of Abelian fields. This research has been subsumed in the book of Urazbaev [72]. An elementary proof for cyclic quartic fields appears in Ou, Williams [01].

A complete solution of the problem of asymptotics for the number of Abelian fields with given Galois group and bounded discriminant was given by Mäki [85]. The same problem for Abelian extensions of an arbitrary algebraic number field has been resolved by Wright [89]. In the case of extensions of prime degree his result was made more precise in H.Cohen, Diaz y Diaz, Olivier [02a] (cf. H.Cohen [00b]).

The number of Abelian fields of a given degree, which have prescribed ramification indices for a fixed set of primes was evaluated in Travesa [90a]. Haberland [74] studied asymptotics of the number of Abelian extensions L/K with a given Galois group, with norms of ramified prime ideals bounded by x.

Similar questions for non-Abelian extensions are much harder to handle. Cubic extensions of arbitrary algebraic number fields have been treated in Datskovsky, Wright [88] (see also Davenport, Heilbronn [69], Roberts [01]. For the quartic case see Baily [80], H.Cohen [03], H.Cohen, Diaz y Diaz, Olivier [00], [02b]. Frobenius fields were considered in Steckel [83] (a general theory of this class of fields was given in Steckel [82b]). For a survey see H.Cohen [02].

Asymptotics for the number of fields of a fixed degree in which the ideal generated by a given rational primes factorizes in a prescribed fashion has been considered in Del Corso, Dvornicich [93].

3. Corollary 1 to Theorem 8.10 goes back to Kummer [50a], [61], [63]. Other special cases of Theorem 8.10 were obtained in Fuchs [66] and Fueter [17], and the general case occurs first in Beeger [19], [20] and Gut [29]. A thorough study of the class-number formula given in that theorem is accomplished in the important book of Hasse [52a].

In special cases the formula given in Theorem 8.10 may be brought to a simpler form. See Hardy, Hudson, Richman, Williams, Holtz [86], [87] for the case of imaginary cyclic quartic fields.

There exist class-number formulas also for other classes of fields. For pure cubic fields such a formula was given by Dedekind [00]. For Abelian extensions of imaginary quadratic fields see Fueter [10], Kubert, S.Lang [81, chap.13], Meyer [57], Novikov [62], [67], Ramachandra [64], [69], Robert [73], Schertz [77].

Hecke [21b] obtained such a formula for the ratio $h(L)/h(K)$ in the case when K is totally real, and $L = K(\sqrt{a})$ with totally positive a. He conjectured that there might exist an elementary formula for that quotient also in the case of totally negative a, and this was confirmed by Goldstein [73b] (except certain particular cases), and Shintani [76b] (cf. Goldstein, de la Torre [75], Reidemeister [22].

If K is real Abelian, then one can express $h(K)$ by indices of certain subgroups of $U(K)$ (Leopoldt [53b], Schertz [79]). These formulas are particularly simple for $K = K_p^+$ in which case $h(K_p^+)$ equals the index of the group

of cyclotomic units in the group of all units of K_p (Kummer [50a,b], [51]; cf. Iwasawa [76], Segal [68], Washington [82]).

Deuring [69] utilized a method of Siegel, developed by Ramanathan [59], to express $h(K)$ by Bessel functions. Modular forms were used in Kiselev [55a] to get a formula for the class-number of cubic fields with negative discriminant.

Landau [04] proved that the Dirichlet series of $\zeta_K(s)/\zeta(s)$ converges at $s = 1$, and this leads to a formula for the product $h(K)R(K)$.

4. The class-number formulas for quadratic fields (Corollary 2 to Theorem 8.10 and Corollary 1 to Proposition 8.12) as well as Proposition 8.12 are due to Dirichlet [38], [39] (whose result covers only the case $4|d(K)$) and Kronecker [85]. They both used the language of quadratic forms. The old problem of finding an elementary proof of these formulas was solved for negative discriminants by Orde [78] (for an exposition see Narkiewicz [86, Chap.V]), and in certain special cases earlier by Davis [76] and Venkov [31]. Mordell [18] found another analytical proof. See Louboutin [02b] for a simple way to compute the class-number of quadratic fields using Dirichlet's formulas.

For short proofs of the fact that the sum appearing in Dirichlet's formulas for $d < 0$ does not vanish see Metsänkylä [77] and Ullom [74b].

Several formulas expressing the class-number for various classes of imaginary quadratic fields by character sums were given in Hudson, Williams [82]. See also the book of Urbanowicz, Williams [00].

For early results on this topic the reader should consult the third volume of Dickson [19].

Other results concerning formulas for the class-number see Barkan [75], Bergström [44], Berndt [73], Berndt, Evans [77], Bitimbaev [68], Bölling [79], Eichler [55], Goldstein, Razar [76], Hasse [40], Hecke [25], [30], [39], Lerch [05], McQuillan [62], Mordell [60b], [64].

Analogues of Proposition 8.12 for zeta-functions of Hecke characters of finite order in a quadratic number field were obtained by Siegel [61] (cf. Rideout [73]). For other fields see King [68], Shintani [77b].

5. Proposition 8.11 is valid for all cyclotomic fields, hence the first factor h_n^- is always an integer. If n is a prime-power, then Kummer asserted that $h^*(K_n^+)$ divides $h^*(K_n) = h(K_n)$, but this fails in general, as the example $n = 100$ shows. Tables of h_n^- were prepared for all n with $\varphi(n) \leq 256$ by Schrutka v.Rechtenstamm [64] (cf. Washington [82]), and for primes $p < 3000$ in Fung, Granville, Williams [92] (cf. Jha [95]). A numerical study of h_p^+ for $p < 10^4$ appears in Schoof [03].

The structure of $H(K_n)$ for all n with $h(K_n) < 10^4$ was determined in Tateyama [82a], where also the structure of the factor group $H(K_p)/H(K_p^+)$ was found for primes $p \leq 227$, with certain exceptions.

The group $H^-(K_n)$ is defined as $\{X \in H(K_n) : \tau(X) = X^{-1}\}$, where $\tau \in Gal(K_n/\mathbb{Q})$ is the complex conjugation. The structure of $H^-(K_p)$, as an

Abelian group and as a Galois module was determined for all primes $p \leq 509$ in Schoof [98]. Cf. Jha [95].

For all primes $p < 10^4$, except $p = 7687$, the 2-class group of K_p is cyclic (Cornacchia [01]).

Corollary 2 to Proposition 8.12 was obtained by Lepistö [69] and Metsänkylä [72], and the proof given by us is due to Metsänkylä [74]. Cf. Carlitz [61], Masley [78b]. For an improvement see Feng [82b], where a bound for $h_{p^n}^-$ was given (cf. Metsänkylä [67a]).

It has been shown in Turnbull [41] and Carlitz, Olson [55] that for odd primes p the Maillet's $p \times p$ determinant

$$\det [R(ij')]_{1 \leq i,j \leq p},$$

(where $R(a)$ denotes the least positive residue of $a \bmod p$, and a' is defined by $aa' \equiv 1 \pmod{p}$) equals $p^{(p-3)/2} h_p^-$. See Carlitz [61], Dohmae [94], Endô [96], Fuchs [97], Galkin [72], Girstmair [93], Hazama [90], Hirabayashi [98], [99], Hyyrö [67], Kanemitsu, Kuzumaki [98], Kučera [01], Kühnova [79], Masley [78b], Metsänkylä [67a], [84], [97], Sands, W.Schwarz [95], W.Schwarz [93], Tateyama [82b], Tsumura [96], [00], K.Wang [84] for various generalizations.

6. A congruence relating h_p^- to Bernoulli numbers was given by Vandiver [18], and a simpler proof was presented in Slavutskii [69] (cf. Hasse [66], Inkeri [55]). Tables of Bernoulli numbers B_{2n} for $n \leq 62$ can be found in Washington [82]. For $63 \leq n \leq 92$ and $91 \leq n \leq 110$ see Davis [35] and Lehmer [36], respectively. A bibliography on Bernoulli numbers was prepared by Skula and Slavutskii [87].

Carlitz [68] determined explicitly an integer $g(p)$ (for odd primes p) such that

$$g(p) h_p^+ \equiv h_p^- \pmod{p}.$$

This implies in particular that $p | h_p^+$ yields $p | h_p^-$, a result of Kummer [50a]. A new proof was given by Metsänkylä [70a], [73], who also generalized Carlitz's congruence, replacing K_p by any its subfield, and regained certain congruences for class-numbers of quadratic fields obtained earlier in Ankeny, Artin, Chowla [52] and Kiselev [48].

7. It was conjectured by Kummer that h_p^- equals asymptotically

$$L(p) = 2p \left(\frac{\sqrt{p}}{2\pi} \right)^{(p-1)/2},$$

and it was shown in Ankeny, Chowla [49], [51] that

$$\log h_p^- = \log L(p) + o(\log p).$$

Cf. Hyyrö [67], Lepistö [63], [66], [68], [74], Masley, Montgomery [76], Metsänkylä [67a], [70a], Pajunen [76], Puchta [00], Siegel [64], Tatuzawa [53].

If q runs over all powers of a prime p then

$$\log h_q^- = (1/4 + o(1))(1 - 1/p)q \log q,$$

as shown by Goldstein [73c].

Recently Murty and Petridis [01] proved that for a certain $c > 0$ and almost all primes p one has

$$\frac{1}{c} < \frac{h_p^-}{L(p)} < c.$$

Earlier Granville [90] showed that this inequality is true for every $c > 0$ and a positive proportion of primes. In the same paper he proved that if Kummer's conjecture is true, then at least one of the following conjectures is false: the conjecture of Hardy and Littlewood, stating that the number of primes $p \leq x$, such that $2p+1$ is also prime, is $\gg x/\log^2 x$, or the conjecture of Elliott-Halberstam, which asserts that for

$$E(x,q) = \max_{(q,a)=1} (\pi(x;q,a) - \frac{\pi(x)}{\phi(x)})$$

one has

$$\sum_{q<x^{1-\epsilon}} |E(x,q)| \ll \frac{x}{\log^M x}$$

for every positive ϵ and $M = 1, 2, \ldots$.

The result of Ankeny and Chowla implies that the equality $h_p^- = 1$ can hold only for finitely many primes p. Uchida [71] proved that this implies $p \leq 19$, and Masley and Montgomery [76] determined all integers $m \not\equiv 2 \pmod 4$ with $h_m^- = 1$ (there are 29 such m's, the largest being 84). The sequence h_p^- grows rather quickly, and already for $p > 229$ one has $h_p^- > 31 \cdot 10^{45}$ (Lepistö [74]; cf. Hoffstein [79]).

It has been shown by Furtwängler [11] that if $p \nmid h_p$, then for all $n \geq 1$ one has $p \nmid h_{p^n}$.

Asymptotical behaviour of h_p is not known. The upper bound

$$h_p < 20 \left(\frac{p}{e}\right)^{(p-2)/2},$$

valid for $p \geq 36$ appears in Slavutskii [86].

The ratio $k(p^n) = h_{p^n}^-/h_{p^{n-1}}^-$ is always an integer, as shown by Westlund [03], and it increases with n for every large fixed prime p (Lepistö [66], [67]). Cf. Girstmair [91], Metsänkylä [69], [72], Morishima [33], [34], Pollaczek [24], Shiratani [67].

Kummer [50a] asserted that if p is an odd prime and $K \subset L \subset \mathbb{Q}(\zeta_p)$, then $h^*(K)$ divides $h^*(L)$. His proof was incorrect, and the first correct proof of this assertion was given by Furtwängler [08]. It was shown by Herbrand [32a] that one can replace here h^* by h.

For other results dealing with divisibility of $h(L)$ by $h(K)$ in case $K \subset L$ see Adachi [73], Fröhlich [57], Honda [60a,b], Inaba [37], Iwasawa [55a], H.Lang [77], Latimer [33], Yokoi [67], [68b], Yokoyama [67].

8. A prime p is called *pseudo-regular*, if p divides h_p, and the p-part of $H(K_p)$ is cyclic. Skula [75] proved that for such primes we have $p \nmid h_p^+$. Earlier (Skula [72]) he established the first case of Fermat's Last Theorem for pseudo-regular exponents. It has been earlier asserted by Vandiver [34] that for this already the condition $p \nmid h_p^+$ suffices, but his proof seems to be incomplete (see Ribenboim [79], p.188). Cf. Dénes [52b], Vandiver [29a].

No prime satisfying $p|h_p^+$ is known, and a conjecture of Vandiver asserts that this never happens. Consequences of this conjecture are discussed in Washington [82] (Ch. 10) (cf. Vandiver [39a,b], [41]). Vandiver's conjecture is equivalent to the statement that for all real Abelian fields K with conductor equal to p one has $p \nmid h(K)$. This is true for cyclic fields of degrees $2, 3, 4$ and 6 (C.Moser [81], Moser, Payan [81]). In Jakubec [94a] a sufficient condition for the truth of Vandiver's conjecture is given in terms of Bernoulli numbers. For generalizations of Vandiver's conjecture see Shiratani [71], Slavutskii [72b], Uehara [75].

The hope that always one has $h_p^+ < p$ was destroyed first in Cornell, Washington [85] under the assumption of GRH, and then in Seah, Washington, Williams [83] with the example $p = 11\,290\,018\,077$. A smaller example, $p = 641\,492$ was found later (Schoof, Washington [88]). In this case one has $h_p^+ = 1\,566\,401$.

Another conjecture states that $h_{2^n}^+ = 1$ holds for all n. See H.Cohn [60] for numerical results on this question. One has always $2 \nmid h(K_{2^n})$ (see e.g. Hasse [52a], [55]).

Shokrollah [99] computed $h^-(K)$ for all Abelian imaginary fields of prime conductor $\leq 10^4$.

It has been proved in Kimura, Horie [87] that for every fixed integer N one has $N|h_n$ for almost all n. The parity of h_n in case when $\omega(n) \leq 3$ can be determined in terms of cyclotomic units (Yoshino [98]).

Divisibility of h^+ for cyclotomic, and, more generally, Abelian fields, by various primes and/or their powers was considered in Cornacchia [97], Estes [89], Jakubec [93], [94b,c], [95], [96a], [97], [98], Kubert [86].

For other results concerning h_n^+ see Ankeny, Chowla, Hasse [65], Dénes [55], Gerth [83a], S.D.Lang [77], Metsänkylä [69], Mirimanoff [91], Morishima [66], Vandiver [29b], Yamaguchi [71].

9. Primes p with $p \nmid h_p^-$ are called *regular*, and the remaining primes are called *irregular*. Kummer [50a] proved that a prime p is irregular if and only if it divides the numerator of a non-zero Bernoulli number with index not exceeding $p - 3$ (cf. Kronecker [56a]), and proved (Kummer [50c]) Fermat's Last Theorem for regular primes.

A similar criterion for $p|h_p^-$, $p^2 \nmid h_p^-$ appears in Kummer [57] (cf. Vandiver [20]). For similar results concerning other classes of fields see Adachi [73], K.S.Brown [74], Coates, Wiles [77], Greenberg [73a], Kudo [75a], Novikov [69], Ribet [76], G.Robert [74], [78], Yager [82]. For a table (with $p < 125\,000$) see Selucký, Skula [81]. It is not known whether there exist infinitely many regular primes. On the other hand, the number of irregular primes is infinite (K.L.Jensen [15]). Small irregular primes have been computed in Wagstaff [78] ($p < 125\,000$), Tanner, Wagstaff [87] ($125\,000 < p < 150\,000$), Ernvall, Metsänkylä [91], [92], and Buhler, Crandall, Sompolski [92] ($p < 10^6$), Buhler, Crandall, Ernvall, Metsänkylä [93] ($10^6 < p < 4 \cdot 10^6$) and Buhler, Crandall, Ernvall, Metsänkylä, Shokrollah [01] ($4 \cdot 10^6 < p < 12 \cdot 10^6$). These computations confirmed the truth of Vandiver's conjecture for primes in the considered range.

One can also consider a generalization of regular primes, using in place of Bernoulli numbers their analogues, associated with Dirichlet characters. The sets of primes obtained in this way are related to the divisibility of class-numbers of cyclotomic fields. See Ernvall [75], [79], Ernvall, Metsänkylä [78], Gut [51a], Kleboth [55], Slavutskii [72a].

Divisibility of h_p^- by primes $\neq p$ was considered in Metsänkylä [67b], [68a,b], [71], and divisibility of $h(K_m)$ and h_m^+ was studied in Lemmermeyer [95a,II].

Ribet [76] strengthened Kummer's criterion, relating the divisibility of Bernoulli numbers by a prime p to the action of the Galois group on the Sylow p-subgroup A_p of $H(K_p)$. There is a canonical decomposition $A_p = \bigoplus_\chi A_\chi$, with χ running over characters mod p. Let X be the unique character mod p satisfying for all $a \not\equiv 0 \pmod p$ the congruence $X(a) \equiv a \pmod{pR_K}$. Ribet's theorem states that for even $k \in [2, p-3]$ the numerator of the k-th Bernoulli number is divisible by p if and only if $A_{X^{1-k}}$ is non-zero. The easier part of this equivalence was proved already by Herbrand [32a]. For other proofs of Ribet's result see Khare [00], Snaith [82]. It has been shown by Soulé [99], who extended an earlier result of Kurihara [92], that $A_{X^{p-k}}$ vanishes for sufficiently large k. Vandiver's conjecture implies that this happens for all k. Cf. also Ernvall [89]. It follows from the results of Mazur and Wiles [84] that one can express the maximal power of p dividing $\#A_\chi$ by generalized Bernoulli numbers (cf. Coates [81], S.Lang [82]). Previous work on this topic was done in Wiles [80] and S.Yamamoto [72]. Another proofs gave Kolyvagin [90], who used Euler systems introduced by him (for an exposition see Rubin [91a]), and Harder, Pink [92]. Euler systems, introduced by Kolyvagin and their generalizations turned out to be a powerful tool in various problems of number theory (see e.g. Rubin [91b], Mazur [93], Nekovář [92], Perrin-Riou [98]). The cardinality of A_χ was studied in Thaine [95].

The number $d(p)$ of Bernoulli numbers B_{2k} ($2 \le 2k \le p-3$) divisible by p is called the *irregularity index* of p. Ribet's theorem implies $C_p^{d(p)} \subset H(K_p)$. One has $d(p) \le p/4$, and the value of $d(p)$ can be determined by solving a

certain system of congruences (Skula [80]). The largest known irregularity index equals 7, and is attained by the prime $p = 3\,238\,481$ (Buhler, Crandall, Ernvall, Metsänkylä, Shokrollah [93]).

10. The Iwasawa theory of $\mathbb{Z}_p$-extensions, developed by Iwasawa in a cycle of papers (Iwasawa [58], [59a,b,c,d], [73a]) brought new life into the theory of cyclotomic fields. For its exposition the reader is referred to the book of Washington [82], or the survey of R.Greenberg [01], and here we point out only certain of its highlights.

Let p be a rational prime. An extension L/K of an algebraic number field K is called a *$\mathbb{Z}_p$-extension*, if it is an infinite normal extension with $Gal(L/K)$ topologically isomorphic to the additive group $\mathbb{Z}_p^+$ of p-adic integers. Here one treats $Gal(L/K)$ as a topological group with Krull topology, a basis of open sets being given by the family $\{Gal(L/k) : [k : K] \text{ finite}\}$. Such an extension is called a *cyclotomic $\mathbb{Z}_p$-extension*, if L is the fixed field of the torsion subgroup of $Gal(M/K)$, where M is obtained by adjoining to K all p^n-th roots of unity ($n = 1, 2, \ldots$). If p is odd and $K = K_p$, then its cyclotomic $\mathbb{Z}_p$-extension coincides with $\bigcup_{n=1}^{\infty} K_{p^n}$.

Iwasawa proved that if L/K is a $\mathbb{Z}_p$-extension, L_n is the unique subfield of L of degree p^n over K, and p^{e_n} is the exact power of p dividing $h(L_n)$, then the equality

$$e_n = \lambda n + \mu p^n + \nu \tag{8.17}$$

holds for sufficiently large n, with constants λ, μ, ν depending on L/K and p.

These constants are still subject to intensive investigation and their behaviour is not yet completely understood. If $K/\mathbb{Q}$ is Abelian, and L/K is a cyclotomic $\mathbb{Z}_p$-extension, then the corresponding constant λ vanishes (Ferrero, Washington [79]. For other proofs see Barsky [83], Sinnott [84]). It has been shown in Babaitsev [80], [81] that for fixed K the coefficient μ is bounded by a value not depending on p or L (cf. Gerth [79a], Greenberg [73b]). On the other hand there exist cyclotomic $\mathbb{Z}_p$-extensions, having μ arbitrary large (Iwasawa [73b]).

R.Greenberg [76] conjectured that both λ and μ vanish for cyclotomic Z_p-extensions of totally real fields. It is known that for every $p \equiv 3 \pmod 4$ there are infinitely many such fields of degree $p - 1$ (Byeon [99b]). For constructions of fields with vanishing λ see Byeon [01b], Fukuda, Komatsu [00], Ichimura, Sumida [97], Kim, Oh [00]. Komatsu [98], [99], Kraft [96], Kubotera [00], Nakagawa, Horie [88], Oh [98], Ozaki, Yamamoto [01], Ozaki, Taya [95], Tang [96], Taya [99]. For particular values of p such constructions were given in Ozaki, Taya [97]. All Abelian fields for which one has $\lambda = \mu = \nu = 0$ were determined by G.Yamamoto [00]. His results imply that Greenberg's conjecture holds for all Abelian fields of prime power degree.

For other results on Iwasawa coefficients see Bloom [79], Candiotti [74], Carroll, Kisilevsky [81], Cuoco [80], Kraft, Schoof [95], Ferrero [77], [78], [80],

Gerth [79b], Gillard [76], Gold [74a], [76b], Greenberg [75], [78], Jehne [59], Kida [80], [82], Kraft [89], Metsänkylä [74], [75a,b], [78], [83], Shiratani [64], Washington [76b].

Washington [75], [78] studied divisibility of $h(L_n)$ by primes $q \neq p$ in a cyclotomic $\mathbb{Z}_p$-extension, and showed that for sufficiently large n the maximal power of q dividing $h(L_n)$ remains constant, and another proof appears in Sinnott [87]. This need not be the case for non-cyclotomic $\mathbb{Z}_p$-extensions. For a generalization see Kisilevsky [97].

For analogues of (8.17) for composites of $\mathbb{Z}_p$-extensions see Bloom, Gerth [81], Cuoco [82], [84], Cuoco, Monsky [81], Friedman [82a,b], Monsky [83].

11. Theorem 8.14 was proved by Siegel [36] for quadratic fields, and by Brauer [47a] for all extension of a fixed degree, not necessarily Abelian or normal. In the second part of his paper Brauer obtained the same assertion for any sequence $\{K_m\}$ of fields, satisfying $[K_m : \mathbb{Q}] = o(\log |d(K_m)|)$. A simple proof of the Siegel-Brauer theorem was found by Pintz [76d]. For other proofs of Siegel's theorem see S.Chowla [50], Chudakov [42], Estermann [48], Goldfeld [74], Heilbronn [38b], Knapowski [68], Linnik [43], [50], Pintz [74], [76c], [77b], Ramachandra [80], Rodosskii [56], Tatuzawa [51].

As observed by Walfisz [36], Siegel's theorem is equivalent to the non-vanishing of $L(s, \chi)$ in the interval $(1 - c(\epsilon)/D^{\epsilon}, 1)$ for every $\epsilon > 0$ and every real character χ, with D being the conductor of χ. Unfortunately, all known proofs of the Siegel-Brauer theorem are ineffective, and so is the constant $c(\epsilon)$ for $\epsilon < 1/2$. In the case $\epsilon = 1/2$ one can get effective results, as shown in Goldfeld, Schinzel [75], Haneke [73], Pintz [76b], [77b]. Stark [74] proved that the Siegel-Brauer theorem can be made effective for a large class of fields, including all fields of a bounded degree which do not have a quadratic subfield (cf. Stark [75c]).

The error term in Theorem 8.14 (and, more generally, in the Siegel-Brauer theorem) can be improved by taking into account the possible real zeros of $\zeta_K(s)$. This was shown by Vinogradov [62], [63a], who proved that if c_K denotes the largest real zero of $\zeta_K(s)$, then for all fields K of a fixed degree we have

$$\log h(K)R(K) = \frac{1}{2} \log |d(K)| + \log(1 - c_K) + O(\log \log |d(K)|).$$

See also Goldfeld [75], Vinogradov [63b].

In the Abelian case Theorem 8.14 was made more precise by Lepistö [70].

12. Corollary 1 to Theorem 8.14 shows that for imaginary quadratic fields K the class-number $h(K)$ tends to infinity with $|d(K)|$. This has been conjectured essentially by Gauss [01], and the first step towards it was made by Hecke. Hecke's proof appeared in Landau [18c]), who deduced it from the Extended Riemann Hypothesis (see Corollary to Lemma 8.15). Essentially the

same result is contained implicitly in Gronwall [13] (see also Chowla, Friedlander [76b], Grosswald [66], Landau [19b], [27b], Mahler [34], Pintz [76a], [77b]). Next Deuring [33] deduced Corollary 2 to Theorem 8.14 from the falsehood of Riemann Hypothesis, and under the same assumption Mordell [34] obtained $h(K) \to \infty$. Chowla [34a] and Landau [18b,c] showed that if there are infinitely many imaginary quadratic fields with a given class-number, then they must be very rare, and finally Heilbronn [34] established the limit relation $h(K) \to \infty$ (cf. Chowla [34d]).

13. All imaginary quadratic fields with even discriminant and class-number one were determined by Landau [03c], and another proof was given by Lerch [03]. The first important step towards the determination of all such fields in the general case was done by Heilbronn and Linfoot [34], who proved that apart of those listed in Proposition 4.44 there can be at most one such field (for another proof see R.G.Ayoub [67]). This follows also from a result of Tatuzawa [51], stating that if $|d(K)|$ exceeds $2100m^2 \log^2(3m)$, then one has $h(K) > m$ with at most one exception (cf. Chowla, Friedlander [76b], Landau [36], Pintz [77b], Ramachandra [75]). Evaluations of the possible tenth discriminant with $h = 1$ (Lehmer [33b], Stark [66]) strengthened the belief that there is no such field, especially in view of the fact that this is implied by *GRH*.

The expected proof was finally found by Baker [66] and Stark [67a,b] (cf. Baker [71a], Stark [69b]). Baker's paper indicated only the method, which was later applied successfully by Bundschuh and Hock [69]. We adopted this approach in the proof of Theorem 8.29.

One should note that an earlier proof of Heegner [52] was known. It was for a long time regarded as erroneous, until Deuring [68] and Stark [69a] provided the needed clarifications (see also Birch [69], Meyer [70], Schertz [76]).

For other proofs of Theorem 8.29 see Cherubini, Wallisser [87], Chowla [70a], Chudakov [69], Feldman, Chudakov [72], Siegel [68b].

14. An effective way of finding all quadratic imaginary fields with class-number 2 was given by Baker [71b] and Stark [71] (cf. Baker, Stark [71]). In the last paper it is shown that for such fields K one has $|d(K)| < 10^{1030}$, and fields in that range have been dealt with in Montgomery, Weinberger [74] and Stark [75b]. It turned out that there are 18 such fields, and they all satisfy $|d(K)| \leq 427$. The case of even discriminants was settled earlier by Weinberger [69] (cf. Baker [69], Ellison et al. [71], Kenku [70]). For an approach based on Heegner's method see Abrashkin [74], Antoniadis [83] and Meyer [75].

The more general question of finding an effective method to determine all imaginary quadratic fields with a given class-number was reduced by Goldfeld [76], [77] to a problem in the theory of elliptic curves, which in turn was solved by Gross and Zagier [83], [86] (for an exposition see Coates [86]). This result

implies the evaluation

$$h(K) \geq C(\epsilon) \log^{1-\epsilon} |d(K)|$$

for every $\epsilon > 0$ with an effective constant $C(\epsilon)$. An exposition was given by Oesterlé [85]. There one can find the explicit lower bound

$$h(K) > C \log D \prod_{\substack{p|D \\ p \neq p_{max}(D)}} \left(1 - \frac{[2\sqrt{p}]}{1+p}\right),$$

where $D = |d(K)|$, $p_{max}(D)$ denotes the maximal prime divisor of D, and C equals $1/55$ if D is not divisible by the prime 5077, and $C = 1/7000$ otherwise (later Buhler, Gross, Zagier [85] provided numerical evidence for the superfluity of the condition on D, and Mestre [85a] eliminated this condition). For a survey see Oesterlé [88].

Using this result all imaginary quadratic fields with $h = 3$ were determined by Oesterlé [85] (the maximal value of $|d(K)|$ being 907 in this case), these with $h = 4$ by Arno [92] (here $|d(K)| \leq 1555$), and the cases $h = 5, 6$ and 7 were resolved by Wagner [96] (with bounds being 2683, 3763 and 5923, respectively). All such fields with odd $h \leq 23$ were determined in Arno, Robinson, Wheeler [98], and recently Watkins [04b] succeeded to cover the range $h \leq 100$. There are over 40 000 such fields K, with the largest $|d(K)|$ being equal to 2 383 747. The maximal number (3283) of fields with a given class-number in this range is attained for $h = 96$.

Buell [99] computed $h(-d)$ for $d \leq 2.2 \cdot 10^9$.

Granville and Stark [00] proved that a form of the ABC-conjecture for number fields implies the inequality

$$h(-d) > \left(\frac{\pi}{3} + o(1)\right) \frac{\sqrt{d}}{\log d} \sum \frac{1}{a},$$

where the sum is taken over all reduced binary quadratic forms $aX^2 + bXY + cY^2$ with $b^2 - 4ac = -d$. Such form is called *reduced*, if $|b| \leq a \leq c$, and if $|b| = a$, or $a = c$, then b is non-negative. See also Conrey, Iwaniec [02] and Sarnak, Zaharescu [02].

15. Corollary 4 to Theorem 8.14 shows that there can be only finitely many complex Abelian fields of given degree and class-number. A much stronger result was proved by Uchida ([71], [72]) who removed the restriction on the degree, and provided the bound $2 \cdot 10^{10}$ for the conductor of such fields with $h = 1$. This lead to a complete determination of all complex Abelian fields with class-number one by Yamamura [92], who showed that there are 172 such fields. Among them 49 are cyclic and the largest occurring conductor is equal to $10921 = 67 \cdot 163$, attained by the field $Q(\sqrt{-67}, \sqrt{-163})$.

For several classes of complex Abelian fields with $h = 1$ full lists were provided earlier. So Uchida [71 II,III] proved that if $p > 19$ is a prime,

then the class-number of the p-th cyclotomic field exceeds 1, and Masley and Montgomery [76] determined all cyclotomic fields with $h = 1$ (a proof may be found in Washington [82], Ch.XI). There are 29 such fields, with conductors bounded by 84. Cf. Hoffstein [79], Lepistö [74], Masley [75], [76], [77], [78a], [79], Metsänkylä [70b]. Complex Abelian quartic fields with $h = 1$ were found in Setzer [80a] (cf. Brown,Parry [74], Goldstein [71b]), and complex Abelian fields of 2-power degree with $h = 1$ in Uchida [88]. For other particular cases see Uchida [72].

There are only finitely many complex Abelian fields with relative class number $h^-(K) = 1$ (Uchida [71,I]), and all 300 such fields were determined in Chang, Kwon [00a]. For sextic fields this has been done earlier in Louboutin [92a]. Later K.Horie [89], [93b] proved that there are only finitely many complex Abelian fields with a given odd part of $h^-(K)$, and listed all cyclotomic fields for which h^- is a power of 2. In Uchida [71,II] it has been observed that it is possible to obtain an explicit upper bound for the conductors of complex Abelian fields K with a given value of $h^-(K)$, with the exception of imaginary quadratic fields and complex biquadratic fields. The structure of $H^-(K)$ for all complex Abelian fields of conductor ≤ 100 was determined in Horie, Ogura [95].

There are only six cyclotomic fields for which the class-group is a non-trivial 2-group (K.Horie [93b]), and two of them, namely K_{39} and K_{56} have class-number two (Masley [75]). All 15 cyclotomic fields with $h \leq 10$ were listed in Masley [76], who also described the structure of their class-groups, except for K_m with $m = 57, 68, 96$ and 120. In the case $m = 68$ F.Gerth III [80] showed that the group is cyclic.

A list of all imaginary biquadratic fields with $h = 2$ was given in Buell, Williams, Williams [77], with $h = 3$ in Jung, Kwon [98], and with $h = 4$ in McCall, Parry, Ranalli [97].

All eight imaginary cyclic quartic fields with $h = 2$ were determined in Hardy, Hudson, Richman, Williams [89], and Louboutin [92b] found all cyclic quartic fields whose class group is of exponent ≤ 2. There are 33 such fields, and the 2-rank of their class-groups is bounded by 3. Cyclic non-quadratic imaginary fields K with $Gal(K/\mathbb{Q})$ being a 2-group and $h^-(K) \leq 20$ were listed in Park, Kwon [98] (there are 169 such fields, their degrees are bounded by 16 and the conductors by 1789).

Lists of all imaginary cyclic fields of degree 2^n with $n \geq 2$, whose class-groups are of the form C_2^N and C_{2^N}, respectively, were given in Louboutin [95a], [97a]. One has $H(K) \sim C_2^N$ (with some N) for 38 such fields, with 33 quartic, four octic and one of degree 16. Cyclic class-groups have 22 fields, and among them there are ten with $h = 1$, nine with $h = 2$ and three with $h = 4$. The finiteness of this set of fields was proved earlier in Horie, Horie [90a,b], where also an upper bound for their conductors was given.

Imaginary cyclic fields with $h \leq 4$ were determined in Chang, Kwon [98].

All imaginary Abelian sextic fields with $h \leq 11$ were found in Park, Kwon [97]. There are 124 such fields.

16. Similar methods can be applied to study CM-fields with a given class-number. It was shown in Uchida [71,I] that the relative class number of a non-Abelian normal CM-field K goes to infinity, when the ratio $[K : Q]/\log|d(K)|$ tends to zero. This result was made explicit in Uchida [73], and later Stark [74] and Odlyzko [75] showed that there can be only finitely many normal CM-fields having a given class-number. Lower bounds for $h^-(K)$ for CM-fields were given in Louboutin [94c].

Hoffstein [79] proved that all normal CM-fields with $h = 1$ have their degrees bounded by 436, and this bound has been reduced by Bessassi [03] to 266, and to 164 under GRH. The following classes of CM-fields with $h = 1$ have been completely determined:

(i) Non-normal quartic (11 fields) and dihedral octic fields (Louboutin, Okazaki [94]) (earlier Louboutin [94a] gave an upper bound for the discriminants of these fields),

(ii) Normal octic with quaternion Galois group (Louboutin [93a]),

(iii) Dihedral (Lefeuvre, [00], Lefeuvre, Louboutin [00], Louboutin, Okazaki, Olivier [97], Louboutin, Okazaki [98]),

(iv) Normal non-Abelian of degree 16 (Louboutin [97b]),

(v) Normal non-Abelian of degree 24 (Lemmermeyer, Louboutin, Okazaki [99], Louboutin [01a], Park [02]),

(vi) Normal non-Abelian of degree 36 (Chang, Kwon [02]),

(viii) Normal non-Abelian of degree 48, having a normal CM-subfield of degree 16. There is only one such field (Chang, Kwon [03]),

(ix) Non-normal sextic (Boutteaux, Louboutin [02a,b]).

There is only one octic CM-field with quaternion Galois group and $h = 2$, namely $Q(i(2+\sqrt{2})^{1/2}(3+\sqrt{6})^{1/2})$ (Louboutin [96a]), and it is not difficult to show that there are no octic quaternion CM-fields with an odd class-number. There is one more octic CM-field with quaternion Galois group for which the exponent of $H(K)$ equals 2 (Louboutin, Okazaki [99]). All non-normal quartic and octic dihedral CM-fields with relative class-number equal 2 have been determined in Yang, Kwon [99]. It was shown in Louboutin [99a] that there are no dicyclic[5] CM-fields of degree $4p$ (with p being an odd prime) of relative class-number one, and in Louboutin, Park [00] all dicyclic CM-fields of degree $4p$ with $h \leq 4$ were found (there are three such fields, all with $p = 3$). A necessary condition for the exponent of the class-group of a CM-field to be ≤ 2 was given in Louboutin [97c].

[5] A group is called *dicyclic*, if it has generators a, b satisfying $a^{2p} = 1$, $a^p = b^2$, $b^{-1}ab = a^{-1}$.

It has been shown in Friedlander [76] that if K is a CM-field with the property that the Dedekind zeta-function of its maximal real subfield vanishes at $s = 1/2$, then for every $\epsilon > 0$ one has

$$h(K) \gg \log^{2-\epsilon}(|d(K)|).$$

All imaginary normal octic fields with $h = 1$ which are not CM-fields have been found by Yamamura [98] (there are 67 such fields).

17. Write, for shortness, $h(d)$ for the class-number of the quadratic field $\mathbb{Q}(\sqrt{d})$. The old question of Gauss [01], whether $h(d) = 1$ holds for infinitely many positive d, is still open. The computer search seems to confirm it. See Takhtayan, Vinogradov [82] for a heuristical approach to this problem.

Using Corollary 2 to Theorem 8.14 and bounds for $L(1, \chi_d)$ (Tatuzawa [51], Hoffstein [80]) one can find all real quadratic fields of the Richaud-Degert type (*R-D* fields) with a given small class-number, with at most one exception (which disappears under GRH). Recall that a field $\mathbb{Q}(\sqrt{D})$ is called an *R-D* field if $D > 0$ is a square-free integer of the form $D = n^2 + r$, where $-n < r \leq n$ and $r|4n$. If one removes the condition $-n < r \leq n$ then one gets the *Extended R-D fields* (ERD fields).

Assuming GRH one can list all ERD fields with class-number one (Mollin, Williams [88a,b]). See also Chowla, Friedlander [76b], Kim, Leu, Ono [87], Lachaud [87], Levesque, Lu [96], Mollin [88], Zhang M.Y. [95].

In certain cases one can eliminate the assumption of GRH. It has been conjectured by Yokoi [86] that if $d = n^2 + 4$ is square-free and $n > 1861$, then $h(d) > 1$. This has been recently proved unconditionally by Biró [03a]. A similar conjecture of Chowla (see Chowla, Friedlander [76a]), stating that if $p = n^2 + 1 > 677$ is a prime, then $h(p) > 1$ was also established by Biró [03b].

Lower bounds for $h(d)$ in the case of *R-D* fields gave Halter-Koch [90a], Mollin [90], Mollin, Williams [91b], Mollin, Zhang , Kemp [94].

In Louboutin, Mollin, Williams [93] a list of 228 ERD fields having class-group of the form C_2^N was presented, and it has been shown that there can be at most one more such field, whose existence would contradict GRH. See also Dohmae [93].

Real quadratic fields $\mathbb{Q}(\sqrt{p})$ with prime $p \equiv 1 \pmod 4$, $h = 1$, and small fundamental units ϵ were considered in Yokoi [90], who proved that the inequality $\epsilon < 2p$ can happen for at most 31 such fields (cf. Katayama, Katayama [94]).

For results relating the class-number of real quadratic fields to continued fractions of the square-root of their discriminants see Dubois, Levesque [91], Louboutin [88], Louboutin, Mollin, Williams [92], Mollin, Williams [89a,b], [90], [91a], [92]. See also the book of Mollin [96d], and the papers quoted there.

All real biquadratic fields $Q(\sqrt{d_1}, \sqrt{d_2})$ with d_1, d_2 of the form $n^2 + 1$ or $n^2 + 4$, and $h \leq 2$ were listed in Katayama, Katayama [92], assuming GRH,

18. Theorem 8.18 is classical (see Dedekind [71]). The proof given by us follows Hecke [23]. For other proofs see Jones [49], König [13], Mitchell [26] (cf. also Butts, Pall [68], Lubelski [36]). Essentially the same argument leads to a correspondence between classes of binary quadratic forms of arbitrary discriminant, and classes of ideals of an appropriate order in a suitable quadratic field. For a good exposition of main properties and applications of orders see Borevich, Shafarevich [64]. The literature on the class-number of binary quadratic forms is quite formidable, and has been reviewed, up to 1922, in the third volume of Dickson [19] by Cresse.

19. Proposition 8.19 appears in Slavutskii [65a,b], and Lemma 8.20, on which its proof rests, is due to Hua [42] (see also Kanemitsu [77]). For prime d the bound in Lemma 8.20 can be improved. In fact, for sufficiently large primes p one has

$$L_p(1) \leq 0.19674 \log p,$$

as shown in Stephens [72]. For another proof see Pintz [77a]. Bounds for $|L(1,\chi)|$ for Dirichlet characters χ were given in a series of papers of Louboutin [93b], and in case of Artin L-functions of Abelian extensions in Louboutin [98a].

The bound in Proposition 8.19 was improved to $h(d) \leq \sqrt{d}/2$ in Le [94].

It is conjectured that with a positive constant C one has $L_d(1) > C/\log d$. Corollary to Lemma 8.15 can be used to deduce this inequality from GRH. This has been first shown by Hecke (see Landau [18c], Mahler [34]). The best known unconditional result is

$$L_d(1) > \frac{C(\epsilon)}{d^\epsilon},$$

holding for every d and $\epsilon > 0$ with a certain positive $C(\epsilon)$. This is a consequence of Siegel's theorem. Hoffstein [80] proved that if $0 < \epsilon < 0.0723$, then for all d with at most one exception (which satisfies $d \geq \exp(1/\epsilon)$)) we have

$$L_d(1) > \min\left\{\frac{0.125}{\log d}, \frac{2.865\epsilon}{d^\epsilon}\right\}.$$

Cf. Gelfond [53], Metsänkylä [70b], Pintz [77b], Tatuzawa [51].

Littlewood [28] showed that under GRH each of the inequalities

$$L_d(1) \leq C \log\log d$$

and

$$L_d(1) \geq \frac{C_1}{\log\log d}$$

holds for infinitely many d with suitable positive C, C_1. Later Chowla [34c] proved the first result unconditionally, and the second was established by Linnik [42] and Walfisz [42]. The first of these inequalities cannot be essentially improved, as for infinitely many d one has $L_d(1) \gg \log\log d$ (Montgomery,

Weinberger [77], cf. Katayama [97]). For large values of $L(1, \chi_d)$ see also Montgomery, Vaughan [99]. It has been shown in Conrey, Iwaniec [02] that certain, yet unproved, assumptions about the spacing of zeros of $\zeta(s)$ imply

$$L_d(1) \geq C(\log d)^{-90},$$

with an computable constant $C > 0$. Sarnak and Zaharescu [02] proved that if Dirichlet's L-function have no non-trivial non-real zeros, then for every $\epsilon > 0$ one has

$$L_d(1) \geq \frac{c(\epsilon)}{\log^{\epsilon} d},$$

and if $\chi_d(-37) = -1$, then for every $\eta > 2/5$ one has

$$L_d(1) \geq \frac{c(\eta)}{d^{\eta}},$$

with an effective constant $c(\eta) > 0$.

20. Let $H(d)$ denote the class-number of primitive binary positive definite quadratic forms of discriminant d. Gauss conjectured that

$$\sum_{n \leq N} H(-4n) = \frac{4\pi}{21\zeta(3)} N^{3/2} - \frac{2}{\pi^2} N + o(N^{3/2}),$$

and this was established by Mertens [74]. The best known evaluation of the error term is $O(N^c)$ with $c = 21/32$ (Chamizo, Iwaniec [98]). These results give the mean value of class-numbers in orders of imaginary quadratic fields. The first result giving the mean value for $h(d)$, d ranging over negative discriminants of quadratic fields, was obtained by Datskovsky [93], who established

$$\sum_{d \leq x} h(-d) = (c + o(1)) x^{3/2},$$

where

$$c = \frac{\pi}{18} \prod_p \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right).$$

In the case of positive discriminants the situation is more complicated. Hooley [84] conjectured that one has

$$S(x) = \sum_{0 < d \leq x} h(d) = \left(\frac{25}{12\pi^2} + o(1)\right) x \log^2 x,$$

and showed that $S(x)$ exceeds $(4/\pi^2) x \log x$. For positive discriminants of quadratic forms asymptotics was obtained in Siegel [44].

Mean values of $H^k(-d)$ and $h^k(-d)$ have been considered in Barban [62], [67], Barban, Gordover [66], Fainleib, Saparniyazov [75], Jutila [73], Lavrik [59], [71a,b], Saparniyazov [65], Stankus [76], Warlimont [71], Wolke [69], [71].

21. Theorem 8.21 is a particular case of the result of Ankeny, Brauer, Chowla [56], who proved that for every $\epsilon > 0$ there exist infinitely many fields K of given signature, satisfying $h(K) \geq |d(K)|^{1/2-\epsilon}$. This was strengthened in Sprindzhuk [74b], where it was shown that this inequality holds for almost all fields of a given degree (see also Sprindzhuk [82]). The result of Montgomery and Weinberger [77], which we already quoted, implies that for real quadratic K the inequality

$$h(K) \geq \sqrt{d}\frac{\log\log d}{\log d}$$

holds for infinitely many $d = d(K)$, and if one believes in GRH, then this is best possible (see also Mallik [81b], Nagell [38]). In another direction Y.Yamamoto [71] obtained $h(K) \ll c\sqrt{d}/\log^2 d$ for infinitely many $d = d(K)$. For a similar result for cubic extensions see Watabe [83].

22. Theorem 8.23 is due to Gauss [01]. See also Arndt [58a], Gogia, Luthar [79], Kronecker [64], Mertens [05], Nemenzo, Wada [92], Reiner [45], Shyr [79]. A deduction of it from the analytical class-number formula was given in Fox, Urbanowicz, Williams [99].

A class-field interpretation of the group $\mathfrak{G}(K)$ of genera of a quadratic field K was given in Hasse [51b], who showed that the maximal unramified extension of K, which is Abelian over $\mathbb{Q}$, coincides with that extension of K which, according to class-field theory, corresponds to $\mathfrak{G}(K)$. This was generalized to cyclic extensions $K/\mathbb{Q}$ in Iyanaga, Tamagawa [51], and to Abelian extensions in Leopoldt [53a] (cf. Gold [75], [76a], Halter-Koch [71c], Hasse [69a], Zhang X. [85]). In this generalization the role of the principal genus is played by

$$\{X^{1-\sigma} : X \in H^*(K), \sigma \in Gal(K/\mathbb{Q})\}.$$

For non-Abelian extensions of the rationals a theory of genera was constructed by Fröhlich [59], [83b]. The genus field of K is defined in this case as the maximal extension of K of the form KL with $L/\mathbb{Q}$ Abelian, which is unramified at finite primes. One can also demand that the genus field is unramified at infinity, which leads to a parallel theory (see Halter-Koch [78b], Horie [83], Stark [76b]). The interested reader should consult the book of M.Ishida [76], as well as the corresponding chapter in G.Gras [03].

23. Using class-field theory one can obtain an analogue of Corollary 1 to Theorem 8.23 for the group $H(K)$ of quadratic K: the group $H(K)$ has $\omega(d) - 1$ even invariants, except in the case when K is real and at least one prime $p \equiv 3 \pmod 4$ is ramified. In this case $H(K)$ has $\omega(d) - 2$ even invariants (see e.g. Herz [66]).

A simple proof of Corollary 2 to Theorem 8.23 was supplied by Takaku [75].

Let $e_p(H), e_p(H^*)$ be the number of invariants of $H(K)$, resp. $H^*(K)$, divisible by the prime p. A simple formula for $e_4 = e_4(H^*)$, in case of quadratic

K, was given in Rédei, Reichardt [34]: let $F(d)$ be the number of factorizations $d = d_1 d_2$, where d_1, d_2 are discriminants of quadratic fields, for which

$$\left(\frac{d_1}{q}\right) = \left(\frac{d_2}{p}\right) = 1$$

holds for all primes p, q, satisfying $p|d_1$ and $q|d_2$. Then $F(d(K)) = 2^{e_4}$. Cf. Hurrelbrink [94], Kisilevsky [82], Lagarias [80c], Rédei [34a,b].

For a similar description of $e_{2^k}(H^*)$ for $k \geq 3$ see Reichardt [34] (cf. Morton [79], [82a,b], [83]). An interesting conjecture concerning the structure of of the 2-part of H^* was proposed in H.Cohn, Lagarias [83] (see also H.Cohn [85]). In certain cases this conjecture was proved by Morton [90] and Stevenhagen [89].

Certain conjectures, concerning the distribution of imaginary quadratic fields with certain types of class-group were presented in H.Cohen [83], H.Cohen, Lenstra [84], and H.Cohen, Martinet [87], [90], where also a heuristic support was given. On these conjectures see also H.Cohen, Martinet [94], Greither [00], Jacobson, Lukes, Williams [95], Lee [02], Stephens, Williams [88], Washington [86], Washington, Zhang X. [97].

For other results concerning the 2-part of $H^*(K)$ for quadratic K see H.Bauer [71], [72], Costa [93], Endô [73a], Halter-Koch [84a], Hasse [69b,c], [70a,b], Kaplan [72], [73a,b], [74], [76], [77b], Lagarias [80a], Moine [72], Oriat [77], [78], Rédei [34c], [36], [38], Reichardt [70], Scholz [35], Waterhouse [73].

Far less is known about $e_p(H)$ for odd p. It is even not known, whether the set of possible values of $e_p(H)$ is unbounded, when K ranges over all quadratic fields, and p over all odd primes.

If $p_1, \ldots, p_k$ are given primes, then there exist infinitely many imaginary quadratic fields K with $e_{p_i}(H(K)) \geq 2$ for $i = 1, 2, \ldots, k$ (Y.Yamamoto [70], Nakano [84]). Moreover $e_3(H) \geq 4$ holds infinitely often both for imaginary (Craig [77]) and real (Diaz y Diaz [78]) quadratic fields. Examples are known of imaginary quadratic fields with $e_3(H) \geq 6$, and real quadratics with $e_3(H) \geq 5$ (Quer [87]; cf. Llorente, Quer [88a]). One has also $e_5(H) \geq 3$ for infinitely many quadratic fields of both signatures (Mestre [92]), and there are examples of imaginary quadratic fields with $e_5(H) \geq 4$ (Schoof [83]; cf. Solderitsch [92]).

The mean value of $e_3(H)$ for quadratic fields was studied in Belabas [99].

24. Invariants of $H(K)$ for arbitrary fields were studied in Rédei [44]. For the case of cyclic fields of prime degree see Inaba [40], [41], and for cyclic fields of prime-power degree see Fröhlich [54b]. An analogue of Corollary 2 to Theorem 8.14 for cyclic fields of prime degree obtained Leopoldt [53a] (cf. Fröhlich [54c], Kuroda [64b], Moriya [30]).

In Armitage, Fröhlich [67] the inequality

$$e_2(H) \geq 2^{r-s} - \left[\frac{r}{2}\right]$$

was established, with $r = r_1(K)$ and s being the number of signatures of units of K.

A formula for $e_3(H)$ for cubic fields was given in Gerth [76c]. Pure cubic fields were treated earlier in Gerth [73], [75a] and Kobayashi [77]. This was generalized by G.Gras [74b] to fields of prime degree p, whose Galois closure has a dihedral Galois group. Cf. Kobayashi [74].

Invariants of the class-group for other classes of fields were treated in Azizi, Mouhib [01], Cornell [83a], Gerth [76a,d], Gras, Moser, Payan [73], Halter-Koch [78c], Kuroda [70], Moriya [30], Oriat [76], Shanks [74], Taylor [75].

25. If $K/\mathbb{Q}$ is Abelian of conductor f and G is its Galois group, then for $a \in [1, f-1]$, $(a, f) = 1$ denote by g_a the restriction to K of the automorphism of $\mathbb{Q}(\zeta_f)$, mapping ζ_f to ζ_f^a. Define an element σ of the group-ring $\mathbb{Z}[G]$ by

$$\sigma = \sum_{1 \le a < f} \frac{a}{f} g_a^{-1},$$

and call the ideal $S = \mathbb{Z}[G] \cap \sigma\mathbb{Z}[G]$ of $\mathbb{Z}[G]$ the *Stickelberger ideal*. It has been proved by Stickelberger [90] in the case $K = \mathbb{Q}(\zeta_p)$ that S annihilates the class-group of K, and the same is true for arbitrary Abelian fields (see e.g. Coates [77], Fröhlich [77b], Washington [89]). If $K = \mathbb{Q}(\zeta_{p^n})$ with odd prime p, and $\tau \in G = Gal(K/\mathbb{Q})$ is the complex conjugation, then the index of the ideal $S \cap (1 - \tau)\mathbb{Z}[G]$ in $\mathbb{Z}[G]$ equals $h^-(K)$, as shown by Iwasawa [62]. Later Sinnott [78] generalized this to all cyclotomic K, in which case this index is of the form $2^a h^-(K)$, with a depending on the $\omega(d(K))$. A further generalization to arbitrary Abelian fields appears in Sinnott [80]. Here additional factors appear, which were studied in Dohmae [97], Kimura, Horie [87]. See Yin [02] for another definition of the Stickelberger ideal. Cf. also C.G.Schmidt [82], [84].

An analogue of Stickelberger's theorem for totally real fields was conjectured by Brumer and proved by Wiles [90b].

Let $K/\mathbb{Q}$ be real Abelian of degree n, let G be its Galois group, and let p be a prime not dividing n. Denote by $C(K)$ the group of cyclotomic units of K, and let $\theta \in \mathbb{Z}[G]$ annihilate the p-part of $U(K)/C(K)$. It follows from Mazur, Wiles [84] that the p-part of $H(K)$ is annihilated by 2θ (for another proof see Thaine [88]). Note that the definition of cyclotomic units used by Thaine was formally distinct from that given in Sinnott [80], however it has been shown in Lettl [90b] and Nóbrega [90] that these definition agree.

Annihilators of the class group of Abelian extensions of imaginary quadratic fields, using elliptic units, were constructed in Rubin [87].

26. Proposition 8.24 is due to Chowla [34b]. It implies in particular that the equality $h(d) = g(d)$ can hold only for finitely many negative discriminants d. Such discriminants are intimately connected with idoneal numbers,

considered already by Euler (see Grosswald [63], Grube [74], Steinig [66]). The smallest known discriminant with $h(d) = g(d)$ equals -1848, and there can be only one more. Moreover it follows from *GRH* (actually it suffices to have $L(53/54, \chi) > 0$ for real characters χ) that the existing list is complete (Chowla, Briggs [54]). For other results on this topic see Hall [37], [39], Hendy [74a], Möller [76a], Swift [48].

Every genus of an imaginary quadratic field contains an ideal of norm not exceeding $B(\epsilon)|d(K)|^{1/4+\epsilon}$ for every $\epsilon > 0$ (Heath-Brown [79]). Previously Baker, Schinzel [71] had the exponent $3/8 + \epsilon$.

The number of imaginary Abelian fields with genus number equal to the class number was shown to be finite in Hamamura [81] and Louboutin [96b]. All non-quadratic fields with this property are known, due to Louboutin [98c], [99b], Miyada [95] and Chang, Kwon [98], [00b].

A quadratic discriminant d is called *regular* (Gauss [01]), if the principal genus in $\mathbb{Q}(\sqrt{d})$ is cyclic. Apparently it is not known, whether there exist infinitely many regular discriminants. See Lippmann [63].

Denote by $m(d)$ the exponent of the group $H^*(K)$ for $K = \mathbb{Q}(\sqrt{d})$, i.e., the order of its biggest cyclic subgroup. Corollary 8 to Proposition 8.24 implies that for negative d the equality $m(d) = 2$ can hold only in finitely many cases. The same applies to discriminants d with $m(d) = 3$ (Boyd, Kisilevsky [72], Weinberger [73a]), $m(d) = 4$ (Earnest, Estes [81]) and $m(d) = 2^k$ for $k \geq 3$ (Earnest, Körner [82]). If one assumes *GRH*, then, as shown in Weinberger [73a], and Boyd, Kisilevsky [72], one has

$$m(d) \gg \frac{\log |d|}{\log \log |d|}$$

for negative d. It has been shown unconditionally in Pappalardi [95] that this holds for almost all d.

Similar questions have been posed also for fields of higher degrees. For certain classes of cubic fields see Louboutin [95b], [97c], [01b], [02a], and for certain quartic fields see Louboutin [94b]. In Louboutin, Okazaki [03] it has been deduced from *GRH* that there are only finitely many *CM*-fields with bounded exponent of the class-group. In the Abelian case this was conjectured by Earnest [87].

27. Theorem 8.25 is due to Nagell [22], whose proof we reproduced. Other proofs were given in Ankeny, Chowla [55], Humbert [40] and Kuroda [64a]. The proof of Kuroda shows that one can also demand $d(K)$ to be divisible by any given integer. Cf. Cowles [80].

The analogue of Theorem 8.25 for real quadratic fields was established by Y.Yamamoto [70], and Fröhlich [57] obtained the same assertion for cyclotomic fields (cf. Osada [87], Weinberger [73b]). For cyclic cubic fields the same assertion was proved in Uchida [74], and for pure cubics in Nakano [83a]. Madan [70] proved the existence of infinitely many normal fields of a given

degree, with $h(K)$ divisible by a given N, and it has been proved in Nakano [84], [85] that there exist infinitely many fields of given degree and signature with $N|h(K)$. For fields with $r_2 \geq 1$ this was done in Azuhata, Ichimura [84].

Divisibility of the class-number of quadratic fields by powers of 2 is closely connected with representations of certain divisors of the discriminant by quadratic forms. The oldest result of this type is contained in a letter of Gauss [28] to Dirichlet, where it is shown that if $p \equiv 1 \pmod 8$ is a prime and $p = x^2 + y^2$, then $h(-4p)$ is divisible by 8 if and only if $x + y \equiv \pm 1 \pmod 8$. On this topic see Barrucand, H.Cohn [69], H.Bauer [72], E.Brown [72], [73], [74a,b], [75], [81], [83], Brown,Parry [73], Costa [93], Hasse [69b,c], [70a,b], Kaplan [72], [73a], Kaplan, Williams, Hardy [86], Koch, Zink [72], Leonard, Williams [82], Pall [69], Reichardt [70], K.S.Williams [76].

Congruences modulo powers of 2 for linear combinations of class-numbers of quadratic fields were treated in the book of Urbanowicz and Williams [00] (cf. G.Gras [89]). There is a large literature about congruences involving class-numbers of quadratic fields. See Carlitz [53a,b], [55], P.Chowla [68], P.Chowla, S.Chowla [68], H.Cohn, Cooke [76], Desnoux [88], Gut, Stünzi [66], Hayashi [77], Hurwitz [95d], Kaplan [77a], [81], Kaplan, Williams [82a,b], [84], Kimura [79b], Kiselev [55b], [59], Kiselev, Slavutskii [59], [62], [64], H.Lang [85a], H.Lang, Schertz [76], Lerch [05], Pizer [76], Pumplün [65], [68], Rédei [28], Schertz [73], Slavutskii [60], [61], [66], K.S.Williams [79], [81a,b,c], [82], Williams, Currie [82].

Similar congruences for class-numbers of other classes of fields have been considered in Carlitz [54], Kudo [75b], Slavutskii [72a].

For divisibility of $h(K)$ by 3 see Belabas, Fouvry [99], Kishi, Miyake [00], Nakagawa, Horie [88], Satgé [79a].

Asymptotical behaviour of the number of imaginary quadratic fields K with $|d(K)| \leq x$ and $p \nmid h(K)$, with a prime $p \geq 5$, was studied in Byeon [99a], Kohnen, Ono [99]. For every prime p there are $\gg_p \frac{\sqrt{x}}{\log x}$ real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with $d \leq x$ such that $p \nmid h(K)$ (Ono [99] under certain additional assumptions, Byeon [01b] unconditionally). A lower bound for the number of $d \leq x$ such that the class-group of $\mathbb{Q}(\sqrt{-d})$ contains an element of a given order q was obtained by M.R.Murty [99], who also proved a similar result in the case of odd q for real quadratic fields. See Soundararajan [00] for an improvement. For a survey of this topic see Kohnen [01].

Densities of sets of quadratic fields (real and/or imaginary) with various restrictions on class-numbers and class-groups were obtained in Gerth [84]. For similar questions for fields of larger degree see Costa, Gerth [95], Gerth [82], [83b,c,d], [86], [87a,b], [89a,b,c], [90], [91].

For other results concerning the divisibility of the class-number of quadratic fields see Chowla, Hartung [74a], Daniel, Fouvry [99], Endô [73b], Fouvry [99], Glaisher [03], Hartung [74a,b], Hayashi [77], Honda [68], Komatsu [01], [02], Oriat [78], Parry [77b], Queen [76], Sase [98], Slavutskii [75], Yamamoto [84].

Similar questions for fields of larger degrees were considered in Barrucand, H.Cohn [70], Callahan [76], H.Cohn [56a], Cornell, Rosen [84], Endô [76], Feng [82c], Frey, Geyer [72], Fröhlich [54a,d], [59], [62c], Furuta [72], Furuya [71], Gerth [76b], Godwin [86], Gold, Madan [78], G.Gras [75], Gras, Gras [75], Greither, Hachami, Kučera [01], Gut [51b], [54], [73], Hayashi [88], Holzer [50], Honda [71], Iimura [71], [79a], Ishida [69], [70], [71], [73], [74], S.Kobayashi [79], [80], Koshi [01], Madan [70], Mollin [83], Montouchet [71], Moriya [30], Morton [83], Nakano [83b], [88], Neumann [73], Ohta [72], [81], Parry [75b,c,d], [78], [80], Parry, Walter [76], Satgé [79a,b], Schertz [78b], [81], Stevenhagen [94a], Uchida [74], [76b], Uehara [82], Wada [70], Walter [80], Washington [87], Watabe [78], [83], Yokoyama [67], Yoshino [97].

28. Theorem 8.27 is due to Brumer [65]. It was strengthened in Roquette, Zassenhaus [69], who gave an elementary proof. Further improvement was done in Connell, Sussman [70]. Corollary 1 to Theorem 8.27 occurs in Fröhlich [62c], and Corollary 4 was proved in Brumer, Rosen [63] (cf. Halter-Koch [81], S.Kobayashi [71], Schmithals [80b]).

Infinitely many fields of any given degree and signature with $C_N^{1+r_2} \subset H(K)$ were constructed in Nakano [84], [85] (cf. Azuhata, Ichimura [84], Ichimura [82], Iimura [79b], Ishida [75], Iwasawa [66], Madan [72], Nakano [86a,b]).

29. Relations between 3-ranks of the class-groups of $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-3m})$ were obtained by Scholz [32]. For other proofs see Martinet, Payan [67], Oriat [76], [77] (cf. Shanks [72]). Oriat's proof is based on the *reflection theorem* proved by Leopoldt [58], which generalizes previous work of Hecke [10], Pollaczek [24] and Takagi [27] (see G.Gras [03]). For other applications of the reflection theorem see G.Gras [72c], [77b], Kudo [72], Oriat [78]. A far-reaching generalization of the reflection theorem gave G.Gras [98].

Relations between 4-ranks of class-groups of quadratic fields were considered in Damey, Payan [70], Gerth [01], Halter-Koch [84a], Sueyoshi [97], Taussky [77b]. For 8-ranks see Bouvier [71], and for 3-ranks for other fields see Callahan [74], Kishi [00].

30. The first result connecting class-numbers of distinct fields is due to Dirichlet [42], who showed that if $k_1 = \mathbb{Q}(\sqrt{m})$, $k_2 = \mathbb{Q}(\sqrt{-m})$ and $K = k_1 k_2$, then

$$h(K) = a h(k_1) h(k_2),$$

where $a = 1$ or $1/2$. See Kubota [56b] for the case of arbitrary biquadratic fields (cf. Halter-Koch [72b]).

Analogues for composites of extensions of prime degree have been proved in Kuroda [50], Litver [49], Pollaczek [29]. For similar results in other classes of fields see Berger [92], Halter-Koch, Moser [78], Inaba [35], N.Moser [79a], Parry [77a], Schertz [74a,b], Schertz, Stender [79], Scholz [30], [33], Värmon [30].

It has been established by Lemmermeyer [95a] that if $K \subset L$ are both CM-fields and $2 \nmid [L : K]$, then h_K^- divides h_L^-. The same holds if $K = Q(\zeta_m) \subset L = Q(\zeta_n)$ (Masley, Montgomery [76]). If $[L : K]$ is even, then this is no more true (there are examples of $h_K^- \nmid 2h_K^-$ in K.Horie [92]), but one has always $h_K^- | 4h_K^-$ (Okazaki [00]).

Relations between the class-groups of a field and its subfields have been studied in Castela [78], G.Gras [74b], Halter-Koch [77], N.Moser [75], Oriat, Satgé [79], Sime [95].

Brauer [51] obtained very general relations between the class-numbers of subfields of a given field. For later development see Jaulent [81d], [82], Jehne [77a], Kuroda [50], Lemmermeyer [94b], Nakagoshi [81], [84], Rehm, Happle [74], Shyr [75], de Smit [01], Walter [77], [79a,b]. For a computational approach see Bosma, de Smit [01].

31. Theorem 8.28 is due to Frobenius [12] and Rabinowitsch [13]. For other proofs see Ayoub, Chowla [81], Connell [62] and Szekeres [74] (cf. Byeon, Dubois, Farhane [99], Stark [02]). Various generalizations of this theorem, giving relations between class-numbers and prime-producing polynomials were given in Byeon, Kim [97], Granville, Mollin [00], Halter-Koch [91], Haneke [69], Hendy [74b], Kim, Hwang [00], Kutsuna [80], Louboutin [89], [90], [91], Louboutin, Mollin, Williams [88], Möller [76b], Mollin [87], [88], [96a,b,c], [97], [98a,b,c], [01], Mollin, Williams [88b], Papkov [44], Sasaki [88], [90], Srinivasan [99]. See also the book of R.A.Mollin [96d].

There are several other conditions related to $h = 1$ in quadratic fields. See Behrbohm, Rédei [36], S.Chowla [61b], [70b], Ennola [58], Lu [79], Mallik [81a], Mitchell [26], Nagell [22], Rédei [60], Zaupper [90].

There are only finitely many polynomials $f_m(X) = X^2 + X + m$ with $m < 0$ with the property that for $x = 0, 1, \ldots, [\sqrt{|m|}] - 1$ the number $|f_m(x)|$ is either prime or equal to 1 (Byeon, Stark [02].

Let $K = \mathbb{Q}(\sqrt{-D})$ with square-free $D > 3$, let $f_D(X) = X^2 + X + (D+1)/4$ if $D \equiv 1 \pmod 4$ and $f_D(X) = X^2 + D$ otherwise, and define the *Ono number* p_D by

$$p_D = \max\{\Omega(f_D(x)) : \ 0 \le x < d(K)\},$$

$\Omega(n)$ denoting the number of prime factors of n, counted with their multiplicities. One can show that $h_D = 1$ is equivalent to $p_D = 1$, and it has been established in Sasaki [86] that one has $p_D \le h(K)$, with equality in the case $h(K) = 2$ (cf. also Möller [76b]) The number p_D has been also studied in Ishibashi [93], Sairaiji, Shimizu [01], [02]. An analogue for real quadratic fields was considered in Sasaki [88].

Interesting relations between the class-number of $\mathbb{Q}(\sqrt{-p})$ and the elements of the period of the continued fraction expansion of $\sqrt{p}$ were for prime p obtained by Hirzebruch [76], and Zagier [75a,b], [81, sect.14]. For related results and conjectures see Chowla, Chowla [72], [73], H.Lang [76], Schinzel [74].

EXERCISES

1. Let $K/\mathbb{Q}$ be Abelian, and let $X(K)$ be the associated group of characters.

(i) For a prime p denote by $a(p)$ the number of characters, whose conductor is a power of p, and which appear in the canonical factorization of at least one character of $X(K)$. Prove that $a(p)$ is equal to the ramification index of a prime ideal lying over p in R_K.

(ii) Determine the decomposition groups and inertia groups of prime ideals of R_K in terms of $X(K)$.

2. For a given $k \geq 3$ determine all prime powers p^N for which there exist primitive characters mod p^N of order k, and find the number of such characters.

3. Characterize integers which are discriminants of cyclic cubic extensions of $\mathbb{Q}$.

4. Find the form of discriminants of Abelian quartic extensions of $\mathbb{Q}$.

5. Determine all subfields of the cyclotomic field K_N, find their discriminants, conductors and generators, with N being your favorite number.

6. (i) Prove that if K is a CM-field, then the index $q(K)$ of $E(K)U(K^+)$ in $U(K)$ equals either 1 or 2.

(ii) Show that if $N \not\equiv 2 \pmod 4$, then $q(K_N)$ equals 1 if and only if N is a prime power.

7. Prove Proposition 8.11 for all cyclotomic fields.

8. (Dirichlet [39], Honda [75], Mordell [61]) Let $p > 3$ be a prime congruent to 3 mod 4.

(i) Prove that for $K = \mathbb{Q}(\sqrt{-p})$ one has

$$h(K) = \frac{1}{a} \sum_{x=1}^{b} \left(\frac{x}{p}\right),$$

where

$$a = 2 - \left(\frac{2}{p}\right), \quad b = \frac{p-1}{2}.$$

(ii) Prove that if $u_p = \pm 1$ satisfies

$$\left(\frac{p-1}{2}\right)! \equiv u_p \pmod p,$$

then $u_p = (-1)^N$, where N is the number of quadratic non-residues mod p in the interval $[1, (p-1)/2]$.

(iii) Deduce Jacobi's conjecture[6]:

$$h(K) \equiv -u_p \pmod 4.$$

9. Let $f(X, Y)$ be a quadratic form of discriminant $d < 0$, lying in the class of forms corresponding to a class A of ideals in $\mathbb{Q}(\sqrt{d})$.

(i) Prove that the set of rational integers represented by f coincides with the set of norms of integral ideals belonging to A^{-1}.

[6] Jacobi [32].

(ii) Show that if $d < -4$, then the number of representations of an integer m by the form f equals the double of the number of integral ideals in A^{-1} having norm m.

10. Find a bound for the function $c(n)$, appearing in Theorem 8.27 in the case $q = 2$.

11. Let f be a quadratic polynomial with rational integral coefficients, let D be its discriminant, and assume that f represents primes at T consecutive integers. Prove that there exists a constant c such that either the roots of f generate a quadratic field with class-number 1, or $T \leq c\sqrt{|D|}$.

9. Factorizations

9.1. Elementary Approach

1. We know already that the condition $h(K) = 1$ is both necessary and sufficient for the uniqueness of factorization in R_K. This shows that fields with trivial class-group can be characterized arithmetically in terms of factorization properties. The discovery made by Carlitz that one can similarly characterize in a simple way fields with class-number 2 gave rise to the thought that it might be possible to obtain a similar description of fields with a given class-number, or class-group. We start with Carlitz's result. To be able to state it we need a simple definition: if $a \in R_K$ is neither zero nor a unit, and $a = \alpha_1 \cdots \alpha_k$ is a factorization of a into irreducible elements of R_K, then k is called the *length* of this factorization.

Theorem 9.1. *If K is an algebraic number field with $h(K) \neq 1$, then for every non-zero and non-unit element $a \in R_K$ all factorizations of a have the same length if and only if $h(K) = 2$.*

Proof : Let $h(K) = 2$, $a \in R_K$, $a \neq 0$ and $a \notin U(K)$. Write

$$aR_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t} \tag{9.1}$$

with distinct prime ideals $\mathfrak{p}_i$, and assume that $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are principal, whereas $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_t$ are not. Then every factorization of a into irreducibles must be of the form

$$a = c_1^{a_1} \cdots c_s^{a_s} d_1 \cdots d_u,$$

where $c_i R_K = \mathfrak{p}_i$ for $i = 1, 2, \ldots, s$, and every d_i generates an ideal of the form $\mathfrak{p}_k \mathfrak{p}_l$ with $k, l > s$. The length of such a factorization equals

$$a_1 + \cdots + a_s + u = a_1 + \cdots + a_s + (a_{s+1} + \cdots + a_t)/2,$$

hence depends only on a, as asserted.

To get the converse implication assume that $h(K) \geq 3$. We have to show the existence of an integer in K with factorizations of distinct lengths. First consider the case when $H(K)$ has an element X of order $g \geq 3$. Corollary 7 to Proposition 7.16 shows that there exist prime ideals $\mathfrak{p} \in X$, $\mathfrak{q} \in X^{-1}$.

The ideals $\mathfrak{p}^g$, $\mathfrak{q}^g$, $\mathfrak{pq}$ are principal, and their corresponding generators a, b, c are irreducible. Since with a certain unit u we have $ab = uc^g$, the number ab has factorizations of lengths $g \geq 3$ and 2. If $H(K)$ is of the form C_2^N and $N \geq 2$, then there are distinct classes $X, Y \in H(K)$ of order 2. Choose prime ideals $\mathfrak{p}_1 \in X$, $\mathfrak{p}_2 \in Y$ and $\mathfrak{p}_3 \in XY$, and observe that the ideals $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_i^2$ $(i = 1, 2, 3)$ are principal, generated by irreducible elements a, b_1, b_2, b_3, respectively. Since with a unit u we have $a^2 = ub_1b_2b_3$, the number a^2 has factorizations of lengths 2 and 3. □

2. Now we prove a purely arithmetic characterization of the class-group, due to Kaczorowski [84a]. To state it we have to introduce certain definitions. If $a \in R_K$ is irreducible, i.e., it cannot be written as a product of two non-unit elements, and all its powers have unique factorization, then a is called *absolutely irreducible*. For every such element a define its *order* $\operatorname{ord} a$ as the maximal rational integer m with the property that with a suitable $b \in R_K$ we have $a | b^m$, $a \nmid b^{m-1}$.

Theorem 9.2. *If $a_1, a_2, \ldots, a_r$ are non-associated absolutely irreducible elements of R_K such that their product has unique factorization, and the sum*

$$\operatorname{ord} a_1 + \operatorname{ord} a_1 + \cdots + \operatorname{ord} a_r$$

is maximal, then

$$H(K) \sim \prod_{i=1}^{r} C_{n_i},$$

where $n_i = \operatorname{ord} a_i$.

Proof : We start with a lemma, which translates the definition of an absolutely irreducible element and its order into ideal-theoretical language:

Lemma 9.3. *An element $a \in R_K$ is absolutely irreducible if and only if $aR_K = \mathfrak{p}^m$ holds for a certain prime ideal $\mathfrak{p}$, lying in a class of order m in $H(K)$. If this condition is satisfied, then $\operatorname{ord} a = m$. In particular, the element a generates a prime ideal if and only if it is absolutely irreducible of order 1.*

Proof : If $aR_K = \mathfrak{p}^m$ holds with a prime ideal $\mathfrak{p}$, whose class is of order m, then a is irreducible, and obviously every power of a has unique factorization, since it cannot be divisible by irreducible elements not associated with a. To show that $\operatorname{ord} a = m$ choose $b \in \mathfrak{p} \setminus \mathfrak{p}^2$, and note that $a | b^m$, $a \nmid b^{m-1}$, hence $\operatorname{ord} a \geq m$. If now $n > m$ and $c \in R_K$ has the property $a | c^n$, $a \nmid c^{n-1}$, then define s by $\mathfrak{p}^s \parallel cR_K$, and observe that $\mathfrak{p}^m | c^n R_K$, $\mathfrak{p}^m \nmid c^{n-1} R_K$, thus

$$(n-1)s < m \leq ns.$$

This implies $s \geq 1$ and we get

$$n-1 \le (n-1)s \le m-1 < n-1,$$

a contradiction. Thus $\operatorname{ord} a = m$.

Now let a be absolutely irreducible, and let (9.1) be the factorization of aR_K into prime ideals. Assume $t \ge 2$ and let g be the order of the class containing $\mathfrak{p}_1$. Then $\mathfrak{p}_1^g$ is principal and generated by b, say. Since b divides a^g, and the ratio a^g/b is not a unit, we may factorize it into irreducibles, say $a^g/b = c_1 \cdots c_r$. But then $a^g = bc_1 \cdots c_t = a \cdots a$ are two factorizations, which are distinct, since at least one of the c_i's lies in $\mathfrak{p}_2$. This contradicts the absolute irreducibility of a, and therefore we must have $t = 1$. But then $aR_K = \mathfrak{p}_1^m$ with a certain $m \ge 1$, and the irreducibility of a implies $m = g$. □

Lemma 9.4. *There exists a constant $B(K)$ with the following property:*

If $a_1, a_2, \ldots, a_r$ are non-associated absolutely irreducible elements of R_K such that their product has unique factorization, and their orders $\operatorname{ord} a_i$ all exceed 1, then

$$\sum_{i=1}^{r} \operatorname{ord} a_i \le B(K),$$

and the class-group $H(K)$ contains a subgroup isomorphic to

$$\prod_{i=1}^{r} C_{n_i} \tag{9.2}$$

with $n_i = \operatorname{ord} a_i$.

Conversely, if $H(K)$ contains a subgroup of the form (9.2), X_i is a generator of C_{n_i}, $\mathfrak{p}_i \in X_i$ is a prime ideal, and

$$\mathfrak{p}_i^{n_i} = a_i R_K \quad (i = 1, 2, \ldots, r),$$

then $a_1, a_2, \ldots, a_r$ are non-associated absolutely irreducible integers, and their product has unique factorization.

Proof : To obtain the first assertion we use the preceding lemma, which implies $a_i = \mathfrak{p}_i^{n_i}$ $(i = 1, 2, \ldots, r)$ with suitable prime ideals $\mathfrak{p}_i$. Denote by X_i the class of $\mathfrak{p}_i$, and observe that the product $\prod_{i=1}^{r} X_i^{c_i}$ (with $0 \le c_i < n_i$) can be equal to the principal class only if all exponents c_i vanish, due to the unique factorization of $a_1 \cdots a_r$. Therefore the classes $X_1, \ldots, X_r$ generate a subgroup of $H(K)$ of the form (9.2). Moreover, we get

$$\sum_{i=1}^{r} \operatorname{ord} a_i = \sum_{i=1}^{r} n_i \le \prod_{i=1}^{r} n_i \le h(K).$$

To get the second assertion it suffices, in view of Lemma 9.3, to show that the product $a_1 \cdots a_r$ has unique factorization. But this follows from the

observation that if c is an irreducible factor of $a_1 \cdots a_r$, non-associated with $a_1, \ldots, a_r$, then

$$cR_K = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$$

holds with $0 \leq b_i \leq n_i$, and for at least one index i we have $0 < b_i \leq n_i$. If now

$$A_i = \begin{cases} 0 & \text{if } b_i = n_i, \\ b_i & \text{otherwise,} \end{cases}$$

then

$$X_1^{A_1} \cdots X_r^{A_r} = E,$$

which is impossible. □

The theorem results now immediately. □

Corollary. *The class-group of K is cyclic of N elements if and only if there exists in R_K an absolutely irreducible element of order N, and for arbitrary non-associated absolutely irreducible elements $a_1, a_2, \ldots, a_r$, whose product has unique factorization, one has*

$$\sum_{i=1}^{r} \operatorname{ord} a_i \leq N. \qquad \square$$

3. Several factorization properties in R_K can be expressed by using elementary combinatorics in finite Abelian groups. We shall show this on the example of irreducibility.

Let A be a finite Abelian group written additively. A non-empty finite system $b = (g_1, g_2, \ldots, g_n)$ of elements of A is called a *block*, if $\sum_{i=1}^{n} g_i = 0$. The number n is called the *length* of b. Two blocks differing only in the ordering are regarded as identical. In the set $\mathfrak{B}(A)$ of all such blocks one defines multiplication by juxtaposition, i.e.,

$$(g_1, g_2, \ldots, g_m)(h_1, h_2, \ldots, h_n) = (g_1, g_2, \ldots, g_m, h_1, h_2, \ldots, h_n).$$

This gives $\mathfrak{B}(A)$ a structure of a commutative semigroup.

A block b is called *irreducible*, if it cannot be written as a product of two blocks. The relevance of this notion to irreducibility of integers in R_K is made clear in the following easy proposition:

Proposition 9.5. *Let $a \in R_K$ be non-zero and non-unit, and let*

$$aR_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are prime ideals, not necessarily distinct, lying in the classes $X_1, \ldots, X_s$ of $H(K)$. The element a is irreducible if and only if the block formed by the classes X_i is irreducible.

Proof : It suffices to observe that every factorization of a, say $a = a_1 a_2$, with

$$a_1 R_K = \mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_k}, \quad a_2 R_K = \mathfrak{p}_{j_1} \cdots \mathfrak{p}_{j_l}$$

induces a factorization of the corresponding block

$$(X_1, \ldots, X_s) = (X_{i_1} \cdots X_{i_k})(X_{j_1} \cdots X_{j_l}),$$

and conversely. □

The *Davenport's constant* $D(A)$ of a finite Abelian group A, written additively, is defined as the smallest integer m with the property that from any sequence of m elements of A one can extract a subsequence with zero sum. This constant is finite and does not exceed the cardinality N of A. Indeed, if $a_1, \ldots, a_N \in A$, then either all elements

$$a_1, a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_N$$

are distinct, and since there are N of them, one must be zero, or two of them are equal, and by subtraction we obtain a non-empty subsequence with vanishing sum.

Proposition 9.6. *The maximal length of an irreducible block in* $\mathfrak{B}(A)$ *equals* $D(A)$.

Proof : Clearly no irreducible block can have its length greater than $D(A)$, so assume that the maximal length of such block is $n < D(A)$. Let $a_1, a_2, \ldots, a_n$ be a sequence in A without a subsequence with vanishing sum, and put $a = -(a_1 + a_2 + \cdots + a_n)$. Then

$$b = (a_1, \ldots, a_n, a)$$

is a block of length $n + 1$, hence it cannot be irreducible. Thus $b = b_1 b_2$ with certain blocks b_1, b_2, but one of the b_i's must be of the form $(a_{i_1}, \ldots, a_{i_r})$, and thus $a_{i_1} + \cdots + a_{i_r} = 0$, which is not possible. □

Corollary. (Davenport) *The maximal number of prime ideal factors of an irreducible element of* R_K *equals* $D(H(K))$.

Proof : Apply Propositions 9.5 and 9.6. □

4. An explicit formula for the value of $D(A)$ is in the general case unknown. Such a formula for p-groups was established by Olson [69] and Schanuel [74]:

Theorem 9.7. *If* p *is a prime and*

$$A = \prod_{i=1}^{t} C_{P_i},$$

where $P_i = p^{n_i}$, *then*

$$D(A) = 1 + \sum_{i=1}^{t}(P_i - 1).$$

Proof : The theorem will result from the following lemma concerning group-rings of finite Abelian p-groups:

Lemma 9.8. *If A is a finite p-group written multiplicatively (with unit element e), which is a product of cyclic groups of orders $P_1, \ldots, P_t$, and if $g_1, \ldots, g_k$ are elements of A with*

$$k \geq 1 + \sum_{i=1}^{t}(P_i - 1),$$

then the element

$$(e - g_1)(e - g_2)\cdots(e - g_k) = \sum_{g \in A} c_g g$$

of the group-ring $\mathbb{Z}[A]$ has all its coefficients c_g divisible by p.

Proof : We may assume that $g_i \neq e$ for $i = 1, 2, \ldots, k$, as otherwise the assertion is evident. If x_i is a fixed generator of C_{P_i}, then write every $g \in A$ in the form

$$g = \prod_{j=1}^{t} x_j^{a_j}, \quad \text{with } 0 \leq a_j < P_j,$$

and define $F(g) = a_1 + \cdots + a_t$.

Now we prove by induction in $\max_j F(g_j)$ that by taking suitable $h_j \in A$ and nonnegative integers M, f_{ij}, satisfying $\sum_{j=1}^{M} f_{ij} = k$, we get

$$\prod_{j=1}^{k}(e - g_j) = \sum_{j=1}^{M} h_j (e - x_1)^{f_{1j}} \cdots (e - x_t)^{f_{tj}}. \tag{9.3}$$

If $\max_j F(g_j) = 1$, then for $j = 1, 2, \ldots, k$ we have $g_j = x_{i_j}$ with suitable i_j, and the assertion holds with $M = h_1 = f_{ij} = 1$. In the general case we can, for $j = 1, 2, \ldots, k$, write $g_j = x_{i_j} t_j$ with suitable i_j and $t_j \in A$, satisfying $F(t_j) = F(g_j) - 1$. In view of the identity

$$e - g_j = (e - x_{i_j}) + x_{i_j}(e - t_j)$$

we get

$$\prod_{j=1}^{k}(e - g_j) = \prod_{j=1}^{k}\left((e - x_{i_j}) + x_{i_j}(e - t_j)\right),$$

and we see that the last product is a sum of terms of the form

$$t\prod_{i=1}^{k}(e-u_i),$$

where $t, u_i \in A$ and $\max_i F(u_i) < \max_j F(g_j)$.

We can thus apply the inductive assumption, except when some of the u_i's are equal to the unit element, but in this case we can just omit the corresponding term.

The equality (9.3) being established, the lemma follows now easily. Indeed, by the assumption imposed on k, for every j at least one exponent f_{ij} in (9.3) satisfies $f_{ij} \geq P_i$. Since

$$(e-x_i)^{P_i} = e + \sum_{k=1}^{P_i-1}\binom{P_i}{k}(-x_i)^k + (-x)^{P_i} = \sum_{j=1}^{P_i-1} s_j x_i^j,$$

with $p|s_j$, we infer that $(1-x_i)^{f_{ij}}$ has all its coefficients divisible by p. In view of (9.3) the same applies to the product $(e-g_1)\cdots(e-g_k)$. □

Now observe that $(e-g_1)\cdots(e-g_k) = \sum_{g\in A} c_g g$, with

$$c_g = \sum_{\substack{2|r\\ g_{i_1}\cdots g_{i_r}=g}} 1 - \sum_{\substack{2\nmid r\\ g_{i_1}\cdots g_{i_r}=g}} 1 + \epsilon_g,$$

where

$$\epsilon_g = \begin{cases} 1 & \text{if } g = e,\\ 0 & \text{otherwise.}\end{cases}$$

The lemma implies $p|c_1$, and if no subsequence of $g_1, \ldots, g_k$ has the unit product, then $c_1 = 1$, a contradiction. Since the g_i's were arbitrary, we get

$$D(A) \leq 1 + \sum_{i=1}^{t}(P_i - 1).$$

To obtain the converse inequality it suffices to consider the sequence of $P_1 + \cdots + P_t - t$ elements, in which a fixed generator x_i of C_{P_i} appears $P_i - 1$ times. □

5. It is also possible to obtain a combinatorial interpretation of the unique factorization. Consider a block $b = (g_1, \ldots, g_k) \in \mathfrak{B}(A)$, and fix the ordering of its elements. If $\alpha:\ b = b_1 \cdots b_t$ is a factorization of b, then we can associate with it a surjective map

$$\Phi_\alpha:\ \{1,2,\ldots,k\} \longrightarrow \{1,2,\ldots,t\},$$

by putting $\Phi_\alpha(i) = j$, if g_i appears in the block j. (From a formal point of view one should consider here rather the sequence of pairs (g_i, i) instead of the

g_i's, but we will not adhere to this pedantic formulation). Two factorizations α, β of b will be called *equivalent* if they have the same number t of factors, and there is a permutation σ of $\{1, 2, \ldots, t\}$ such that the sets

$$\{i : \Phi_\alpha(i) = j\}, \quad \text{and } \{i : \Phi_\beta(i) = j\}$$

coincide for $j = 1, 2, \ldots, t$. A block b is said to have a *unique factorization* if all its factorizations into irreducible blocks are equivalent. Note that this property is independent of the ordering of elements of b.

Proposition 9.9. *If $(X_1, \ldots, X_k)$ is a block in $\mathfrak{B}(H(K))$ which has unique factorization, then for every choice of prime ideals $\mathfrak{p}_i \in X_i$ $(i = 1, 2, \ldots, k)$ any generator of the principal ideal $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$ has unique factorization in R_K.*

Moreover, if $a \in R_K$ has unique factorization, and $aR_K = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ with distinct prime ideals $\mathfrak{p}_i$, then the block in $\mathfrak{B}(H(K))$ formed by the classes of $\mathfrak{p}_i$'s has unique factorization.

Proof : If $aR_K = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ with $\mathfrak{p}_i \in X_i$, then every factorization of the block $b = (X_1, \ldots, X_k)$ induces a factorization of a. In fact, if α is a factorization of b, then $a = a_1 \cdots a_r$ with

$$a_j R_K = \prod_{s=1}^{c_j} \mathfrak{p}_{m(j,s)},$$

where $c_1 + \cdots + c_r = k$, and for every j we have

$$\{m(j, s) : 1 \leq s \leq c_j\} = \{i : \Phi_\alpha(i) = j\}.$$

One sees that every factorization of a into irreducibles is induced in this way by a factorization of b, and different factorizations of a are induced by inequivalent factorizations of b. If all prime ideals $\mathfrak{p}_i$ are distinct, then, conversely, inequivalent factorizations of b induce distinct factorizations of a. □

Note that the second assertion of Proposition 9.9 may fail to hold if aR_K is not a product of distinct prime ideals. For instance, if $H(K) = C_2$, and $b = (a_1, a_2, a_3, a_4)$, where $a_1 = a_2 = a_3 = a_4$ is the non-unit element of $H(K)$, then the factorizations $b = (a_1a_2)(a_3a_4)$ and $b = (a_1a_3)(a_2a_4)$ are inequivalent. However, if $\mathfrak{p}$ is a non-principal prime ideal in R_K, and $aR_K = \mathfrak{p}^2$, then the element $b = a^2$ has unique factorization.

Denote by $a_1(A)$ the maximal length of a block in $\mathfrak{B}(A)$ which has unique factorization, and does not contain the unit element. Note that if the group A is non-trivial, then $a_1(A)$ is finite, because if $b = b_1 \cdots b_s$ is a unique factorization of b into irreducible blocks, then no element of A can appear in two distinct b_i's. Thus $s \leq \#A$, and since the length of each b_i does not exceed $D(A)$ by Proposition 9.6, we get $a_1(A) \leq D(A) \cdot \#A$.

For non-zero $a \in R_K$ denote by $s(a)$ the number of distinct non-principal prime ideals dividing aR_K.

Corollary. *If $H(K)$ is non-trivial, then for every element $a \in R_K$ having unique factorization we have $s(a) \leq a_1(H(K))$, and there is an element a with unique factorization, for which equality holds.*

Proof : The second part of the assertion results from the proposition, as well as the first part in the particular case when the ideal aR_K is square-free, i.e., is a product of distinct prime ideals. It remains to show that the inequality $s(a) \leq a_1(H(K))$ holds also for these a with unique factorization which generate a non-square-free ideal.

Let a be such an element, and let (9.1) be the factorization of aR_K into prime ideals. We may assume that all ideals $\mathfrak{p}_i$ are non-principal, i.e., $t = s(a)$. Assume that the ideals $\mathfrak{p}_j^{a_j}$ are principal for $j = 1, 2, \ldots, r$ and non-principal for $j \geq 1 + r$, and denote by X_j the class of $H(K)$ containing $\mathfrak{p}_j$ (if $j \leq r$), resp. $\mathfrak{p}_j^{a_j}$ (if $j \geq 1 + r$). Thus all classes X_i are non-principal. Choose prime ideals $\mathfrak{q}_i \in X_i$ for $i = 1, 2, \ldots, t$, and $\mathfrak{Q}_i \in X_i^{-1}$ for $i = 1, 2, \ldots, r$, so that they are all distinct, and observe that the ideal $\mathfrak{q}_1 \cdots \mathfrak{q}_t \mathfrak{Q}_1 \cdots \mathfrak{Q}_r$ is principal. Let b be one of its generators. To prove our assertion it suffices to show that b has unique factorization, since the ideal generated by b is square-free, and as the assertion has been already proved in this particular case, we get

$$s(a) = t \leq t + r = s(b) \leq a_1(H(K)).$$

If the order of X_i equals m_i, and π_i is, for $i = 1, 2, \ldots, r$, a generator of $\mathfrak{p}_i^{m_i}$, then m_i divides a_i. If we put $A_i = a_i/m_i$, then the number

$$c = \prod_{i=1}^{r} \pi_i^{A_i}$$

has unique factorization, being a divisor of a, and this implies that the classes $X_1, \ldots, X_r$ generate independent cyclic subgroups of $H(K)$. Indeed, if with suitable $0 \leq \alpha_i < m_i$ we would have

$$\prod_{i=1}^{r} X_i^{\alpha_i} = E,$$

then the product $\prod_{j=1}^{r} \pi_j^{\alpha_j}$ would be principal, equal to λR_K, say, and λ would have unique factorization, being a divisor of c. This is, however, impossible, as $\pi_j \nmid \lambda$ for $j = 1, 2, \ldots, r$, and $\lambda \mid \prod_{j=1}^{r} \pi_j$.

Denote by G the subgroup of $H(K)$, generated by $X_1, \ldots, X_r$, and observe that no product $Y = X_{i_1} \cdots X_{i_k} \neq E$ with $r + 1 \leq i_1 < i_2 < \ldots < i_k \leq t$ can lie in G. Indeed, if this were the case, then with suitable $0 \leq b_j < m_j$ $(j = 1, 2, \ldots, r)$ we would have $Y = \prod_{i=1}^{r} X_i^{b_i}$, and thus the ideal

$$\mathfrak{p}_1^{a_1-b_1}\cdots\mathfrak{p}_r^{a_r-b_r}\mathfrak{p}_{i_1}^{a_{i_1}}\cdots\mathfrak{p}_{i_k}^{a_{i_k}}$$

would be principal. Its generator, being a divisor of a, would have unique factorization, and this would lead to $m_j|b_j$ and $b_j = 0$ for $j = 1, 2, \ldots, r$.

It follows now immediately that b has unique factorization. □

6. Now we shall present another combinatorial constant, related to the question of unique factorization of rational integers in quadratic fields.

Let A be a finite Abelian group written multiplicatively. Denote by $M(A)$ the maximal cardinality of a subset $\{a_1, \ldots, a_n\}$ of A with the property that all products

$$\prod_{j=1}^{n} a_j^{\epsilon_j} \quad (\epsilon_j = 0, 1; j = 1, 2, \ldots, n)$$

are distinct.

To establish a link between $M(A)$ and factorizations consider a quadratic number field K, and observe that if $X \in H(K)$, then the orbit of X under the action of the Galois group of $K/\mathbb{Q}$ equals (X, X^{-1}). Indeed, if $\mathfrak{p} \in X$ is a prime ideal of first degree, and $\mathfrak{p}'$ is its conjugate, then by Theorems 4.6 and 4.39 we have $\mathfrak{p}' \in X^{-1}$. From each orbit $\neq (E, E)$ (with E being the unit class) choose one class, let $\mathcal{X} = \{X_1, \ldots, X_t\}$ be the set of classes obtained in this way, and let O_i be the orbit (X_i, X_i^{-1}). If p is a rational prime such that $pR_K = \mathfrak{p}_1\mathfrak{p}_2$, with $\mathfrak{p}_1 \in X_i$, $\mathfrak{p}_2 \in X^{-1}$, then we shall say that p *belongs to the orbit* O_i, and write $p \vdash O_i$.

Proposition 9.10. *Suppose that* $O_{i_1}, \ldots, O_{i_s}$ *are distinct orbits* $\neq (E, E)$ *and let* $p_j \vdash O_j$ *for* $j = 1, 2, \ldots, s$. *Then the number* $m = \prod_{i=1}^{s} p_i$ *has unique factorization in* K *if and only if all products*

$$\prod_{j=1}^{s} X_{i_j}^{\epsilon_j} \tag{9.4}$$

with $\epsilon_j \in \{0, 1\}$ *are distinct.*

Proof : By Proposition 9.9 the number m has unique factorization if and only if the block $b = (X_{i_1}, X_{i_1}^{-1}, \ldots, X_{i_s}, X_{i_s}^{-1})$ has unique factorization in $\mathfrak{B}(H(K))$. Since all blocks (X_i, X_i^{-1}) are irreducible, this happens if and only if b has no irreducible factor of length exceeding 2. Observe now that if

$$(X_{k_1}, \ldots, X_{k_l}, X_{r_1}^{-1}, \ldots, X_{r_m}^{-1}) \tag{9.5}$$

with $\{k_1, \ldots, k_l, r_1, \ldots, r_m\} \subset \{i_1, i_2 \ldots, i_s\}$ is such a factor, then for all $t \neq u$ we have $k_t \neq k_u$, and

$$X_{k_1}\cdots X_{k_l} = X_{r_1}\cdots X_{r_m}, \tag{9.6}$$

showing that not all products (9.4) are distinct. Conversely, if two products of the form (9.4) are equal, then after suitable cancellation we arrive at an equality of the form (9.6), showing that the block in (9.5) does not have an irreducible factor of length 2, i.e., of the form (X, X^{-1}) □

Corollary. *If m is a square-free rational integer having unique factorization in a quadratic number field K, then m can have at most $M = M(H(K))$ prime factors which do not generate prime ideals, and do not split into principal factors in K.*

Moreover, there exist integers m, for which this bound is attained.

Proof : Observe first that if $m = p_1 \cdots p_s$ has unique factorization in K, and the primes p_i are distinct, then they must belong to different orbits. Indeed, if, for example, p_1 and p_2 belong to the same orbit (X, X^{-1}), then by Proposition 9.9 their product cannot have unique factorization. We may thus apply the last proposition to get $s \leq M$. To show that this bound is attained, observe that if $Y_1, \ldots, Y_M$ are classes in $H(K)$ such that all products

$$\prod_{j=1}^{M} Y_j^{\epsilon_j}$$

with $\epsilon_j = 0$ or 1 are distinct, then for $i \neq j$ we have $Y_i Y_j \neq E$. Thus all orbits (Y_i, Y_i^{-1}) are distinct. If now $p_i \vdash (Y_i, Y_i^{-1})$ for $i = 1, 2, \ldots, M$, then it follows from the proposition that the product $p_1 \cdots p_M$ has unique factorization in K. □

Our next result gives certain information about the size of $M(A)$.

Proposition 9.11. *If A is a direct product of the cyclic groups $C_{n_1}, \ldots, C_{n_r}$, then*

$$\sum_{j=1}^{r} \left[\frac{\log n_j}{\log 2} \right] \leq M(A) \leq \frac{\log \#A}{\log 2}.$$

Proof : The upper bound results from the fact that number of zero-one sequences of length M equals 2^M. The lower bound is obtained by considering for $j = 1, 2, \ldots, r$ the elements

$$X_j, X_j^2, X_j^{2^2}, \ldots, X_j^{2^{k_j}},$$

where X_j is a generator of C_{n_j}, and k_j is the largest integer satisfying

$$1 + 2 + 2^2 + \cdots + 2^{k_j} < n_j. \qquad \square$$

Corollary. *If A is either cyclic, or a 2-group, then*

$$M(A) = \frac{\log \# A}{\log 2}. \qquad \square$$

7. *Elasticity* of factorizations $\rho(R)$ in a domain R is defined as the least number c such that for every non-zero and non-unit element $x \in R$ if

$$x = \alpha_1 \cdots a_m = b_1 \cdots b_n$$

with irreducible factors, then $n/m \leq c$. In the case of algebraic number fields this constant is related to the Davenport's constant of the class-group.

Proposition 9.12. *One has* $\rho(R_K) = D(H(K))/2$,

Proof : Put $D = D(H(K)$, and let $X_1, \ldots, X_D \in H(K)$ be classes, forming an irreducible block of maximal length. For $i = 1, 2, \ldots, D$ choose prime ideals $\mathfrak{p}_i, \mathfrak{q}_i \in X_i$, and observe that with certain $\alpha, \beta, \gamma_1, \ldots, \gamma_D$ we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_D = \alpha R_K, \mathfrak{q}_1 \cdots \mathfrak{q}_D = \beta R_K, \mathfrak{p}_i \mathfrak{q}_i = \gamma_i R_K.$$

The resulting equality $\alpha\beta = \epsilon\gamma_1 \cdots \gamma_D$ (with a unit ϵ) leads now to $\rho(R_K) \geq D/2$.

On the other hand, assume that with certain $k \geq l$ we have an equality $\alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ where $\alpha_i, \beta_j \in R_K$ are irreducible elements, none of which generates a prime ideal. By Corollary to Proposition 9.6 the number of prime ideal factors of the right-hand side of this equality does not exceed lD, and that of the left-hand side is at least equal to $2k$. Therefore we get $2k \geq lD$, thus $k/l \leq D/2$, and $\rho(R_K) \leq D/2$. $\square$

9.2. Quantitative Results

1. In this section we shall consider counting functions of irreducible integers and integers with unique factorization, and start with an auxiliary result concerning the distribution of ideals having a prescribed number of prime ideal divisors in a given class of $H(K)$.

Let X be a given set of ideals. We shall denote by $\omega_X(I)$ the number of distinct prime ideals belonging to X which divide the ideal I, and by $\Omega_X(I)$ the number of these prime ideals, counted with their multiplicities. In other words, we put

$$\Omega_X(\mathfrak{p}^m) = \begin{cases} m & \text{if } \mathfrak{p} \in X, \\ 0 & \text{otherwise,} \end{cases}$$

and extend Ω_X to all ideals I by additivity, i.e.,

$$\Omega_X(I) = \sum_{\mathfrak{p}^m \| I} \Omega_X(\mathfrak{p}^m).$$

Theorem 9.13. *Let $X_1, \dots, X_m$ be given classes in $H(K)$, and let $c_1, \dots, c_m$ be given non-negative integers. We assume that in the case $m = h(K)$ not all c_i vanish. For $i = 1, 2, \dots, m$ let the function f_i be equal to either ω_{X_i} or Ω_{X_i}, and denote by $\Phi(x) = \Phi(x; f_1, \dots, f_m; c_1, \dots, c_m)$ the number of ideals I of R_K, satisfying $N(I) \le x$ and $f_i(I) = c_i$ for $i = 1, 2, \dots, m$. Finally, let $\Phi_Y(x) = \Phi_Y(x; f_1, \dots, f_m; c_1, \dots, c_m; Y)$ be the number of such ideals lying in a given class Y of a certain group $H_{\mathfrak{f}}^*(K)$. Then, for x tending to infinity, we have*

$$\Phi(x) = \begin{cases} (C + o(1))x \log^{-m/h} x (\log\log x)^T & \text{if } m < h, \\ (C_1 + o(1))x \log^{-1} x (\log\log x)^{T-1} & \text{if } m = h, \end{cases}$$

where $h = h(K)$, $T = c_1 + \cdots + c_m$, and C, C_1 are positive constants, defined by

$$C^{-1} = \gamma c_1! \cdots c_m! h^T \Gamma\left(1 - \frac{m}{h}\right),$$

and

$$C_1^{-1} = \gamma c_1! \cdots c_m! \frac{h^T}{T},$$

where $\gamma > 0$ depends only on $X_1, \dots, X_m$.

Moreover, if $m < h/2$, then

$$\Phi_Y(x) = (h_{\mathfrak{f}}^*(K)^{-1} + o(1))\Phi(x).$$

Note that the constants C, C_1 do not depend on the choice of the functions f_i.

Proof : Let χ be a character of $H_{\mathfrak{f}}^*(K)$, and consider the function

$$H_\chi(s; z_1, \dots, z_m) = \sum_I \frac{(\prod_{j=1}^m z_j^{f_j(I)})\chi(I)}{N(I)^s}, \tag{9.7}$$

defined for $\operatorname{Re} s > 1$ and $|z_i| \le 1$ $(i = 1, 2, \dots, m)$. By Lemma 7.1 we can write, using the expansion of the logarithm,

$$H_\chi(s; z_1, \dots, z_m) = \prod_{\mathfrak{p}} \left(1 + \sum_{j=1}^{\infty} \left(\prod_{i=1}^m z_i^{f_i(\mathfrak{p}^j)}\right) \chi(\mathfrak{p})^j N(\mathfrak{p})^{-js}\right)$$

$$= \exp\left(\sum_{\mathfrak{p}} \log\left((1 + \sum_{j=1}^{\infty} \left(\prod_{i=1}^m z_i^{f_i(\mathfrak{p}^j)}\right) \chi(\mathfrak{p})^j N(\mathfrak{p})^{-js}\right)\right) = ABC,$$

where

$$A = \exp\left(\sum_{\mathfrak{p}}\left(\prod_{i=1}^{m} z_i^{f_i(\mathfrak{p}^j)}\right)\chi(\mathfrak{p})(\mathfrak{p})^{-s}\right),$$

$$B = \exp\left(\sum_{\mathfrak{p}}\sum_{j\geq 2}\left(\prod_{i=1}^{m} z_i^{f_i(\mathfrak{p}^j)}\right)\chi(\mathfrak{p})^j(\mathfrak{p})^{-js}\right)$$

and

$$C = \exp\left(\sum_{\mathfrak{p}}\sum_{k\geq 2}\frac{(-1)^{k+1}}{k}\left(\sum_{j=1}^{\infty}\left(\prod_{i=1}^{m} z_i^{f_i(\mathfrak{p}^j)}\right)\chi(\mathfrak{p})^j(\mathfrak{p})^{-js}\right)^k\right).$$

Write, for shortness, $X' = \bigcup_{j=1}^{m} X_j$, $H_{\mathfrak{f}}^* = H_{\mathfrak{f}}^*(K)$ and $h_{\mathfrak{f}}^* = h_{\mathfrak{f}}^*(K)$. Since $f_j(\mathfrak{p}) = 1$ for $\mathfrak{p} \in X_j$, and $f_j(\mathfrak{p}) = 0$ otherwise, Corollary 6 to Proposition 7.16 implies

$$\begin{aligned}\log A &= \sum_{Z\in H_{\mathfrak{f}}^*}\chi(Z)\left(\sum_{j=1}^{m} z_j \sum_{\mathfrak{p}\in X_j\cap Z}\frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}\in Z\setminus X'}\frac{1}{N(\mathfrak{p})^s}\right)\\ &= \frac{1}{h_{\mathfrak{f}}^*}\sum_{Z\in H_{\mathfrak{f}}^*}\chi(Z)\left(\sum_{j=1}^{m}(a(Z,X_j)-1)z_j + 1\right)\log\frac{1}{s-1}\\ &\quad + g_\chi(s; z_1, \ldots, z_m),\end{aligned}$$

where

$$a(Z, X_j) = \begin{cases} 1 & \text{if } Z \subset X_j,\\ 0 & \text{otherwise,}\end{cases}$$

and g_χ is a function regular in Re $s \geq 1$. Observe that g_χ does not depend on the choice of the functions f_i, and, in particular, $\alpha = g_{\chi_0}(1; 0, \ldots, 0)$ (where χ_0 is the principal character) depends only on the classes $X_1, \ldots, X_m$.

Now put

$$d_j(\chi) = \frac{1}{h_{\mathfrak{f}}^*}\sum_{Z\in H_{\mathfrak{f}}^*}\chi(Z)a(Z, X_j),$$

and for non-principal χ put $R(\chi) = \sum_{j=1}^{m} d_j(\chi)$, observe that $d(\chi_0) = 1/h(K)$, and note that the product BC is a function regular in Re $s \geq 1$ for $|z_j| \leq 1$.

With these notations we obtain

$$\begin{aligned}&H_{\chi_0}(s; z_1, \ldots, z_m)\\ &= \prod_{j=1}^{m}\exp\left(\frac{z_j}{h}\log\frac{1}{s-1}\right)(s-1)^{m/h}h_{\chi_0}(s; z_1, \ldots, z_m),\end{aligned} \tag{9.8}$$

with h_{χ_0} regular for Re $s \geq 1$ and $|z_j| \leq 1$. Similarly, for non-principal χ we get the equality

$$H_\chi(s; z_1, \dots, z_m)$$
$$= \prod_{j=1}^{m} \exp\left(z_j d_j(\chi) \log \frac{1}{s-1}\right) (s-1)^{R(\chi)} h_\chi(s; z_1, \dots, z_m). \tag{9.9}$$

Observe now that for $\chi = \chi_0$ the product AB attains at $s = 1$, $z_1 = \dots = z_m = 0$ a non-zero value, and therefore we get $\gamma = h_{\chi_0}(1; 0, \dots, 0) \neq 0$. Note also that this value does not depend on the choice of $f_1, \dots, f_m$.

Expanding the right-hand sides of (9.8) and (9.9) into power series in $z_1, \dots, z_m$, and comparing coefficients in (9.7) we arrive at the following equalities, valid for Re $s > 1$:

$$\sum_{\substack{(I,\mathfrak{f})=1 \\ f_i(I)=c_i, i=1,\dots,m}} N(I)^{-s}$$
$$= (s-1)^{m/h-1} \sum_{\substack{r_i+j_i=c_i \\ i=1,\dots,m}} A^{(\chi_0)}_{r_1,\dots,r_m} \frac{1}{h^J} \prod_{i=1}^{m} (j_i!)^{-1} \log^J \frac{1}{s-1} + G_{\chi_0}(s), \tag{9.10}$$

and

$$\sum_{\substack{(I,\mathfrak{f})=1 \\ f_i(I)=c_i, i=1,\dots,m}} \chi(I) N(I)^{-s}$$
$$= (s-1)^{R(\chi)} \sum_{\substack{r_i+j_i=c_i \\ i=1,\dots,m}} A^{(\chi)}_{r_1,\dots,r_m} \prod_{i=1}^{m} d_i^{j_i}(\chi) \prod_{i=1}^{m} (j_i!)^{-1} \log^J \frac{1}{s-1} + G_\chi(s),$$

where $J = j_1 + \dots + j_m$, G_χ are regular for Re $s \geq 1$, and the functions $A^{(\chi)}_{r_1,\dots,r_m}$ are defined by

$$\sum_{r_1,\dots,r_m} A^{(\chi)}_{r_1,\dots,r_m} z_1^{r_1} \cdots z_m^{r_m} = h_\chi(s; z_1, \dots, z_m).$$

Note that $A^{(\chi_0)}_{0,\dots,0} = \gamma$.

Applying to the equality (9.10) Theorem I of Appendix II in the case $\mathfrak{f} = R_K$, we get the first two assertions of the theorem.

To obtain the last assertion we again use (9.10). Write for Re $s > 1$

$$\sum_{\substack{I \in Y \\ f_i(I)=c_i, i=1,\dots,m}} N(I)^{-s} = \frac{1}{h^*_\mathfrak{f}} \sum_{\chi} \overline{\chi(Y)} \sum_{\substack{I \\ f_i(I)=c_i, i=1,\dots,m}} N(I)^{-s} \chi(I) N(I)^{-s}$$
$$= (s-1)^{m/h-1} P_0\left(\log \frac{1}{s-1}\right) + \sum_{\chi \neq \chi_0} (s-1)^{R(\chi)} P_\chi\left(\log \frac{1}{s-1}\right) + g(s),$$

where P_0, P_χ are polynomials with coefficients regular in Re $s \geq 1$, and g regular in that half-plane. The degree of P_0 equals $c_1 + \dots + c_m = T$, and its leading coefficient does not vanish at $s = 1$. Finally, we have

$$\text{Re}\,(-R(\chi)) = -\text{Re}\left(\frac{1}{h_{\mathfrak{f}}^*}\sum_{i=1}^{m}\sum_{Z\in H_{\mathfrak{f}}^*}\chi(Z)a(Z,X_i)\right)$$

$$\leq \frac{1}{h_{\mathfrak{f}}^*}\sum_{i=1}^{m}\sum_{Z\in H_{\mathfrak{f}}^*}a(Z,X_i) = m/h < 1 - m/h,$$

and we may again apply Theorem I of Appendix II. □

Note that in the last part of the theorem one cannot omit the condition $m < h/2$. Indeed, if $h = 2$, $\mathfrak{f} = R_K$, $Y = E$ and $X_1 \neq E$, then for $f_1 = \Omega_{X_1}$ and odd c_1 we get $F_Y(x) = 0$ for all x.

Corollary 1. *If $A(x,n)$, $B(x,n)$ denote the number of ideals I with $N(I) \leq x$, which have n prime ideal divisors, resp. n prime ideal factors counted according to their multiplicities, then with a certain positive constant C one has*

$$A(x,n) = (C + o(1))\frac{x(\log\log x)^{n-1}}{\log x},$$

and

$$B(x,n) = (1 + o(1))A(x,n).$$

Proof : Observe that if $H(K) = \{X_1,\ldots,X_h\}$, then for $m = h(K)$ and $f_i = \omega_{X_i}$, resp. $f_i = \Omega_{X_i}$ the sum

$$\sum_{\substack{c_1,\ldots,c_h\\ c_1+\cdots+c_h=n}} \Phi(x;c_1,\ldots,c_h)$$

equals $A(x,n)$, resp. $B(x,n)$ and apply the theorem. □

Corollary 2. *For the number of principal ideals I with $N(I) \leq x$, which have n prime ideal factors counted with their multiplicities one has*

$$(C_1 + o(1))\frac{x(\log\log x)^{n-1}}{\log x},$$

with certain $C_1 > 0$.

Proof : If $X_1,\ldots,X_h$ are all classes in $H(K)$, then the number in question equals

$$\sum_{\substack{c_1+\cdots+c_h=n\\ X_1^{c_1}\cdots X_h^{c_h}=E}} \Phi(x;c_1,\ldots,c_h),$$

where in the definition of Φ only the functions Ω_{X_i} are involved. Now it suffices to apply the theorem. □

Corollary 3. *Let $X_1, \dots, X_h$ be all classes in $H(K)$, and let $c_1, \dots, c_h$ be given, not all vanishing. Then the number of ideals $I \in X_j$ with $N(I) \leq x$ and $\Omega_{X_i}(I) = c_i$ for $i = 1, 2, \dots, h$, equals*

$$(C_2 + o(1)) \frac{x(\log\log x)^{T-1}}{\log x},$$

with positive C_2, and $T = c_1 + \cdots + c_h$, if $\prod_{i=1}^{h} X_i^{c_i} = X_j$, and $T = 0$ otherwise.

Proof: Observe that if $\prod_{i=1}^{h} X_i^{c_i} = X_j$, then every ideal I satisfying $\Omega_{X_i}(I) = c_i$ for $i = 1, 2, \dots, m$ lies in X_i, and apply the theorem. □

Note finally that the same method as used in the proof of Theorem 9.13 leads to the proof of the following result:

Proposition 9.14. *Let $\Pi_1, \dots, \Pi_m$ be disjoint regular sets of prime ideals having positive densities $a_1, \dots, a_m$. Let for each $i = 1, 2, \dots, m$ a function f_i be given, which equals either ω_{Π_i} or Ω_{Π_i}. Further, let $c_1, \dots, c_m$ be given non-negative integers with non-vanishing sum T, and let $F(x; c_1, \dots, c_m)$ be the number of ideals I with $N(I) \leq x$, and $f_i(I) = c_i$ for $i = 1, 2, \dots, m$. Then*

$$F(x; c_1, \dots, m) = (C + o(1)) x (\log x \log x)^M \log^{-a} x,$$

where

$$a = \sum_{j=1}^{m} a_j, \quad M = \begin{cases} T & \text{if } a < 1, \\ T - 1 & \text{if } a = 1, \end{cases}$$

and C is a positive number, not depending on the choice of the functions f_i.

We leave the needed modifications to the reader.

2. Our next application of Theorem 9.13 concerns irreducible integers:

Theorem 9.15. *Let $F(x)$ be the number of pairwise non-associated irreducible integers in K whose norms do not exceed x in absolute value. Then*

$$F(x) = (C + o(1)) \frac{x(\log x \log x)^{D-1}}{\log x}$$

with a suitable $C > 0$ and $D = D(H(K))$.

Proof : If $I = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ is a principal ideal, $\mathfrak{p}_i$ are prime ideals, not necessarily distinct, and X_i is the class of $\mathfrak{p}_i$ in $H(K)$, then let $b(I)$ be the block $(X_1, X_2, \dots, X_s)$ in $\mathfrak{B}(H(K))$. Let $b_1, \dots, b_r$ be all irreducible blocks in $\mathfrak{B}(H(K))$. By Proposition 9.5 we have

$$F(x) = \sum_{j=1}^{r} \sum_{\substack{I \in E, N(I) \le x \\ b(I) = b_j}} 1.$$

Now, if for a class X we denote by $c_j(X)$ the number of appearances of X in b_j, then $b(I) = b_j$ holds if and only if for every class X we have $\Omega_X(I) = c_j(X)$. This shows that in view of Corollary 3 to Theorem 9.13 we have, in the notation of Theorem 9.13,

$$\begin{aligned} \sum_{\substack{I \in E, N(I) \le x \\ b(I) = b_j}} 1 &= \Phi_E(x; \{c_j(X) : X \in H(K)\}) \\ &= (C + o(1)) \frac{x (\log\log x)^{t_j - 1}}{\log x}, \end{aligned}$$

with $t_j = \sum_{X \in H(K)} c_j(X)$ being the length of the block b_j. An application of Proposition 9.6 leads now to the assertion. □

One can also ask for rational primes which remain irreducible in K. Such primes exist rather seldom, as the following easy result shows:

Proposition 9.16. *Let $K/\mathbb{Q}$ be normal, and assume that there are rational primes which do not ramify in $K/\mathbb{Q}$, and which remain irreducible in K. Then the Galois group of $K/\mathbb{Q}$ contains a cyclic subgroup of index not exceeding $D(H(K))$.*

Proof : If p does not ramify in $K/\mathbb{Q}$, then we have $pR_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ with distinct prime ideals $\mathfrak{p}_i$. If X_i is the class of $\mathfrak{p}_i$ in $H(K)$, then by Proposition 9.5 the block $(X_1, \ldots, X_s)$ is irreducible and so, by Proposition 9.6, we have $s \le D(H(K))$. However, by Corollary to Proposition 6.8, s is the index of the decomposition group of $\mathfrak{p}_1$ in $Gal(K/\mathbb{Q})$, and since the decomposition group is cyclic, the result follows. □

Corollary 2 to Theorem 7.29 shows that if $K/\mathbb{Q}$ is cyclic of degree N, then infinitely many rational primes generate prime ideals in R_K, and Theorem 7.30 implies that the density of the set of all these primes equals $\varphi(N)/N$, because a cyclic group of order N has $\varphi(N)$ generators. There may be also other primes which remain irreducible. In the special case of cyclic extensions of prime degree we shall now prove a formula expressing the asymptotic behaviour of their counting function:

Proposition 9.17. *Let $K/\mathbb{Q}$ be cyclic of prime degree q, and denote by $P(x)$ the number of rational primes $p \le x$ which remain irreducible in K. Then*

$$P(x) = (c + o(1)) \frac{x}{\log x},$$

where

$$c = 1 - \frac{1}{q} + \frac{1}{h(K)} \sum_{b \in A} r(b),$$

A denotes the set of all irreducible blocks in $\mathfrak{B}(H(K))$, which are invariant under the action of $G = Gal(K/\mathbb{Q})$, and for every such block the number $r(b)$ is defined by

$$r(b) = \begin{cases} 1/q & \text{if all classes in } b \text{ coincide,} \\ 1 & \text{otherwise.} \end{cases}$$

Proof : As in the proof of Theorem 9.15, we have

$$P(x) = \sum_{b \in A} \sum_{\substack{p \le x \\ b(pR_K) = b}} 1 + \sum_{\substack{p \le x \\ pR_K \text{ is prime}}} 1.$$

In order to evaluate the inner sum in the first term observe that if $b = (X_1, \ldots, X_r)$ and $X_1 = X_2$, then necessarily $X_1 = X_2 = \ldots = X_r$, as G is cyclic of prime degree. Thus the classes in b are either all distinct, or all equal. Using Corollary 4 to Proposition 7.17 we get in the first case

$$\sum_{\substack{p \le x \\ b(pR_K) = b}} 1 = \sum_{\substack{\mathfrak{p} \in X_1 \\ N(\mathfrak{p}) \le x}} 1 = \left(\frac{1}{h(K)} + o(1) \right) \frac{x}{\log x} = (r(b) + o(1)) \frac{x}{\log x},$$

and in the second case

$$\sum_{\substack{p \le x \\ b(pR_K) = b}} 1 = \frac{1}{q} \sum_{\substack{\mathfrak{p} \in X_1 \\ N(\mathfrak{p}) \le x}} 1 = \left(\frac{1}{qh(K)} + o(1) \right) \frac{x}{\log x} = (r(b) + o(1)) \frac{x}{\log x}.$$

Adding these equalities, and noting that in virtue of Corollary 5 to Proposition 7.16 one has

$$\sum_{\substack{p \le x \\ pR_K \text{ is prime}}} 1 = \left(1 - \frac{1}{q} + o(1) \right) \frac{x}{\log x},$$

we obtain our assertion. □

3. Now we turn to numbers with unique factorization. In this subsection $F(x)$ denotes the number of non-associated integers $\alpha \in K$ with $|N(\alpha)| \le x$ having unique factorization. We shall determine the right order of magnitude of $F(x)$, however, we will not prove the corresponding asymptotic equality, whose available proof is rather technical.

Theorem 9.18. *Let K be an algebraic number field with $h = h(K) \ge 2$. Then*

$$x(\log\log x)^a (\log x)^{1/h-1} \ll F(x) \ll x(\log\log x)^a (\log x)^{1/h-1},$$

with $a = a_1(H(K))$, as defined in Subsect. 5 of the preceding section.

Proof : Let $A = \{b_1, \dots, b_k\}$ be the set of all blocks in $\mathfrak{B}(H(K))$ which have unique factorization, and do not contain the unit class E. Since the length of a block in A does not exceed a, the set A is finite. If now $X_1, \dots, X_{h-1}$ are the non-unit classes of $H(K)$, and $c_j(X_i)$ denotes, as in the proof of Theorem 9.15, the number of occurrences of X_i in the block b_j, then by Proposition 9.9 and Theorem 9.13 we get

$$\begin{aligned} F(x) &\geq \sum_{j=1}^{k} \sum_{\substack{I \in E, N(I) \leq x \\ \Omega_{X_i}(I) = c_j(X_i), i=1,\dots,h-1}} 1 \\ &= (C_1 + o(1)) x (\log\log x)^a (\log x)^{1/h-1}, \end{aligned}$$

with a suitable positive C_1. This proves the first part of the assertion. To prove the second, we utilize Corollary to Proposition 9.9, from which we obtain immediately

$$\begin{aligned} F(x) &\leq \sum_{\substack{c_1,\dots,c_{h-1} \\ \sum c_j \leq a}} \sum_{\substack{I \in E, N(I) \leq x \\ \Omega_{X_i}(I) = c_i, i=1,\dots,h-1}} 1 \leq \sum_{\substack{c_1,\dots,c_{h-1} \\ \sum c_j \leq a}} \sum_{\substack{N(I) \leq x \\ \Omega_{X_i}(I) = c_i, i=1,\dots,h-1}} 1 \\ &= (C_2 + o(1)) x (\log\log x)^a (\log x)^{1/h-1}, \end{aligned}$$

with a certain C_2, the final inequality being a consequence of Theorem 9.12. □

This theorem shows that the class-number measures in some sense the deviation of the ring R_K from a ring with unique factorization, since it shows that the asymptotic order of the counting function of non-associated integers with unique factorization diminishes with the growth of the class-number.

A set $\mathcal{X}$ of element of R_K consisting of full classes of associated integers is said to contain *almost all integers* of K, if its counting function

$$\mathcal{X}(x) = \#\{a \in \mathcal{X} : \ a \text{ pairwise non-associated}, \ |N(a)| \leq x\}$$

satisfies

$$\lim_{x \to \infty} \frac{\mathcal{X}(x)}{I(x)} = 1,$$

where $I(x)$ denotes the number of pairwise non-associated integers a with $|N(a)| \leq x$. Clearly $I(x)$ equals the number of principal ideals of R_K with norms not exceeding x, and thus by Theorem 7.18 we have $I(x) = \kappa x + o(x)$, with κ defined by (6.8). Thus $\mathcal{X}$ contains almost all integers if and only if $T(x)/x$ tends to κ, when x tends to infinity. Similarly, we say that $\mathcal{X}$ contains almost no integers if $\mathcal{X}(x) = o(x)$. Using this terminology we can state a simple corollary:

Corollary. *If $h(K) \geq 2$, then almost no integer of K has unique factorization.* □

4. It is possible to obtain a similar result for the number $F_0(x)$ of positive rational integers $n \leq x$, having unique factorization in a given field K. The proof in the general case relies on class-field theory, and so we treat here only the simplest case of cyclic extensions of prime degree.

Theorem 9.19. *Let $K/\mathbb{Q}$ be cyclic of prime degree q, and let $h = h(K) \geq 2$. Then with a certain positive constant C one has*

$$F_0(x) = (C + o(1))x(\log\log x)^M(\log x)^{(1-h)/hq},$$

where M is a non-negative integer depending on the action of the Galois group of $K/\mathbb{Q}$ on $H(K)$, and not exceeding the number of orbits distinct from $(E, E, \ldots, E)$. If $q = 2$, then $M = M(H(K))$, as defined in Subsect.6 of the preceding section.

Proof: Let $O_1, \ldots, O_r$ be all orbits $\neq (E, E, \ldots, E)$ of $H(K)$ under the action of the Galois group of $K/\mathbb{Q}$. With every orbit $O_i = (X_1, \ldots, X_q)$ we associate the set $\mathfrak{P}_i$ consisting of all rational primes p for which $pR_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ holds with prime ideals $\mathfrak{p}_i \in X_i$. Note that every rational prime, which does not generate a prime ideal in K, lies in one of the sets $\mathfrak{P}_i$. If the orbits $O_1, \ldots, O_t$ have the form $(X, X, \ldots, X)$, and the remaining $r - t$ orbits consist of distinct classes, then Corollary 6 to Proposition 7.16 shows that the sets $\mathfrak{P}_i$ are regular, and their density equals

$$d(\mathfrak{P}_i) = \begin{cases} \frac{1}{hq} & \text{if } 1 \leq i \leq t, \\ \frac{1}{h} & \text{if } t < i \leq r. \end{cases}$$

We need the following simple observation:

Lemma 9.20. *If a rational integer n has unique factorization in K, then n cannot have two distinct prime divisors belonging to the same set $\mathfrak{P}_i$.*

Proof: Let n be a rational integer having two divisors $p_1, p_2 \in \mathfrak{P}_i$, we see that

$$p_1 R_K = \prod_{i=1}^{q} \mathfrak{p}_i, \quad p_2 R_K = \prod_{i=1}^{q} \mathfrak{p}_i'$$

holds with suitable prime ideals $\mathfrak{p}_i, \mathfrak{p}_i' \in X_j$, and thus $p_1 p_2$ has two factorizations arising from

$$p_1 p_2 R_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_q)(\mathfrak{p}_1' \cdots \mathfrak{p}_q') = (\mathfrak{p}_1' \mathfrak{p}_2 \cdots \mathfrak{p}_q)(\mathfrak{p}_1 \mathfrak{p}_2' \cdots \mathfrak{p}_q). \qquad \square$$

Let now $\mathcal{A}$ be the set of all sequences $(a_1, \dots, \alpha_r)$ with the property that there exists a square-free rational integer n with unique factorization in K, for which $\omega_{\mathfrak{P}_i}(n) = a_i$ holds for $i = 1, 2, \dots, r$. Lemma 9.20 shows that $a_i \in \{0, 1\}$, and therefore the number

$$M = \max\{\sum_{j=1}^{r} a_j : (a_1, \dots, a_r) \in \mathcal{A}\}$$

does not exceed r.

Finally, note that if n satisfies $\Omega_{\mathfrak{P}_i}(n) = a_i$ for $i = 1, 2, \dots, r$, and $(a_1, \dots, a_r) \in \mathcal{A}$, then, owing to Proposition 9.9, n has unique factorization in K. This leads to

$$\sum_{(a_1,\dots,a_r)\in\mathcal{A}} \sum_{\substack{n\le x \\ \Omega_{\mathfrak{P}_i}(n)=a_i, i=1,\dots,r}} 1 \le F_0(x) \le \sum_{(a_1,\dots,a_r)\in\mathcal{A}} \sum_{\substack{n\le x \\ \omega_{\mathfrak{P}_i}(n)=a_i, i=1,\dots,r}} 1,$$

and an application of Proposition 9.14 gives the assertion. If $q = 2$, then Corollary 2 to Proposition 9.10 implies $M = M(H(K))$. □

In the general case we prove only the following simple result:

Proposition 9.21. *If $K/\mathbb{Q}$ is normal of degree N and $h = h(K) \ge 2$, then with a suitable $B \ge 0$ we have*

$$F_0(x) \ll x(\log\log x)^B (\log x)^{(1-h)/hN}.$$

Proof : Let $\mathfrak{P}$ be the set of all rational primes which do not ramify in $K/\mathbb{Q}$, and which have a non-principal ideal factor of degree 1 in R_K. In view of

$$\sum_{p\in\mathfrak{P}} \frac{1}{p^s} = \frac{1}{N} \sum_{\substack{\mathfrak{p}\nmid E \\ f_{K/\mathbb{Q}}(\mathfrak{p})=e_{K/\mathbb{Q}}(\mathfrak{p})=1}} \frac{1}{N(\mathfrak{P})^s} \quad (\mathrm{Re}\ s > 1),$$

we infer by Corollary 6 to Proposition 7.16 that $\mathfrak{P}$ is regular and has density $(h-1)/hN$. Now assume that $n \in \mathbb{Z}$ has unique factorization in K. Lemma 9.20 shows that n cannot be divisible by two primes, each of which has a prime ideal divisor in the same class of $H(K)$, and this implies that $\omega_{\mathfrak{P}}(n)$ does not exceed the number of distinct orbits $\neq (E, \dots, E)$ of $H(K)$ under the Galois group of $K/\mathbb{Q}$. Denoting this number by B, and applying Proposition 9.14 we get our assertion. □

9.3. Notes to Chapter 9

1. Theorem 9.1 is due to Carlitz [60]. It is not true for arbitrary Dedekind domains, as suitable counterexamples can be constructed using the results of Claborn [68]. Domains in which Theorem 9.1 holds are called *half-factorial domains* (HFD). Half-factorial domains and related semigroups were studied first by Skula [76] and Zaks [76], [80]. In Coykendall [99] it has been proved that if an order in an algebraic number field is HFD, so is its integral closure. Note that a localization of a Dedekind HFD domain may be not HFD, as an example given in Anderson, Chapman, Smith [94] shows. Orders in quadratic number fields which are HFD's were described by Halter-Koch [83] and Coykendall [01]. There is a large literature concerning HFD, and a survey was given in Chapman, Coykendall [00]. For some variants of HFD see Chapman, Smith [90a], [92a,b].

Other characterizations of algebraic number fields with particular class-groups have been given in Chapman, Smith [90b], Czogała [81], Di Franco, Pace [85], Feng [85], Geroldinger [90d,I], Kaczorowski [81a], Krause [84]. Salce, Zanardo [82].

Theorem 9.2 is due to Kaczorowski [84a]. A variant of it was given in Halter-Koch [83], where also another elementary description of $H(K)$ was presented (cf. Halter-Koch [90b]). Yet another description appears in Rush [83]. For a unified treatment see Geroldinger [90d,II].

Absolutely irreducible elements were studied in Kaczorowski [81b], [84b].

2. Theorem 9.7 was proved by Olson [69] and Schanuel [74]. For further results concerning Davenport's constant $D(A)$ see Baayen [69], Baayen, Emde Boas, Kruyswijk [69], Chapman [95], Delorme, Ordaz, Quiroz [01], Emde Boas [69], Emde Boas, Kruyswijk [67], Gao [00], Geroldinger, Schneider [92].

The constant $M(A)$ appears, in the special case $A = C_k^n$, already in Shannon [56]. It is easy to see that $M(C_3^n) = n$, and in Mead, Narkiewicz [82] the equality $M(C_5^n) = 2n$ has been established, and the value of $M(C_m^2)$ was found for certain integers m. The bound given in Proposition 9.11 was for $A = C_k^n$ improved by S.K.Stein [77].

Combinatorial constants occurring in Sect.1 have been considered in Narkiewicz [79] and Narkiewicz, Śliwa [82]. For these and other combinatorial constants related to factorizations see Chapman [95], Gao [97], Gao, Geroldinger [98], Geroldinger [97a,b], [98], Geroldinger, Kaczorowski [92], Geroldinger, Lettl [90], Halter-Koch [92a], Hassler [03], Krause, Zahlten [91], W.A.Schmid [03a], Skula [76], Śliwa [76a], [82b]. For a more general approach to block semigroups see Geroldinger [94], Halter-Koch [92c,d], W.A.Schmid [03b].

3. Proposition 9.12 appears in Steffan [86]. Elasticity in various classes of domains has been studied in Anderson, Anderson [92], Anderson, Anderson,

Chapman, Smith [95], Anderson, Chapman [00], Cahen, Chabert [95], Chapman, Smith [90a], [93b], Gonzalez [99], Valenza [90]. It can be considered also in certain semigroups (Halter-Koch [95]).

4. Theorems 9.13 and 9.15 are due to Rémond [66] (cf. Lardon [71]). An evaluation of the error term in Theorem 9.4 and an asymptotical expansion was given in Kaczorowski [83], where also one finds corresponding expansions for counting functions considered in Theorems 9.15 and 9.19. An extension of Theorem 9.13 appears in Śliwa [76a]. Corollary 1 to that theorem is due to Nakamura [59]. It has been shown in Halter-Koch, Müller [91] that the constant in Theorem 9.15 depends only on the class-group of the field.

The condition given in Proposition 9.16 for the existence of unramified primes which remain irreducible in K is necessary, but, in general, not sufficient. In the case of normal extensions a necessary and sufficient condition was given in Śliwa [77]. For the case of a cyclic extension of prime degree see Wegner [32b].

4. The first result dealing with asymptotics of functions related to factorizations is due to Fogels [43], who established Corollary to Theorem 9.18 for the field $\mathbb{Q}(\sqrt{-5})$. In 1962 Turán asked me, whether one can obtain the same assertion in the general case, and this has been done in Narkiewicz [64]. In Theorem 9.19 one has in fact $C_1 = C_2$, hence there is an asymptotic equality (Narkiewicz [72]). Theorem 9.19 was proved in the case $q = 2$ in Narkiewicz [66], and Odoni [76] obtained asymptotics for $F_0(x)$ for arbitrary, not necessarily normal, fields in the form

$$(a(K) + O(1/\log\log x))\frac{x(\log\log x)^{b(K)}}{\log^{c(K)} x},$$

where $a(K) > 0$, $0 \leq b(K) < 1$ and $c(K) < h(K)$. An analogous result for the counting function of rational integers with at most m factorizations was obtained by Śliwa [76b]. Asymptotics for the number of elements of R_K with at most k factorizations was studied in Halter-Koch, Müller [91], and Geroldinger, Halter-Koch [92a] (see also Halter-Koch [93b]).

Another approach to the count of irreducible integers and integers with at most m factorizations was presented by Helmut Weber [84], who used a method of Siegel.

If $h(K) \geq 3$, then almost all integers of K have factorizations of distinct lengths, and the same applies to rational integers (Narkiewicz [66]). Asymptotics for the counting function of numbers with at most k factorization lengths was obtained in both cases in Śliwa [76a] (cf. Geroldinger [90a], [91], Halter-Koch, Müller [91], Śliwa [82b]).

Rosiński and Śliwa [76] settled in the negative a question of Turán, who asked whether the function $f_K(n)$, counting factorizations of a rational integer n in a given field K with $h(K) \geq 2$ can have a non-decreasing normal

order. (Recall that a function $F(n)$ is called a *normal order* for f, if the inequality

$$|f(n) - F(n)| < \epsilon F(n)$$

holds for every positive ϵ and almost all n). The function $\log f_K(n)$ has a nondecreasing normal order, equal to $c(K) \log\log n \log\log\log n$ with a certain $c(K) > 0$ (Narkiewicz [80]). Similarly, the function $c_1(K) \log\log n$ (with $c_1(K) > 0$) serves as a normal order for the number of factorizations of n in K with distinct lengths, provided $h(K) \geq 3$. This was proved independently in Allen, Pleasants [80], and Narkiewicz, Śliwa [78].

Asymptotics for $\sum_{n \leq x} f_K(n)$ was found by Rémond [66]. A formula for the number of distinct factorizations in the case of class-number 2 was derived (in a more general setting of Krull monoids) in Chapman, Herr, Rooney [99], and the number of factorizations of distinct lengths was determined in the case $D(H(K)) \leq 4$ in McCoy, Parry [90].

Asymptotics for several counting functions related to factorization properties in orders of global fields was obtained in Geroldinger, Halter-Koch, Kaczorowski [95]. A more general approach, covering also algebraic function fields, was developed in Halter-Koch, Müller [91].

5. It has been proved by Geroldinger [88] that the set of all lengths of factorizations of a given element is essentially a union of finite arithmetical progressions, and for almost all elements it forms a finite arithmetic progression (cf. Geroldinger [90c]). The same holds also, more generally, in a class of Krull domains (Geroldinger [97c]), and in certain monoids (Geroldinger [98]). Cf. Freiman, Geroldinger [00], Gao, Geroldinger [00], Halter-Koch [93a]. Elements for which the set of factorization lengths forms a finite arithmetic progression was studied in Geroldinger [89]. For lengths of factorizations see also Geroldinger, Halter-Koch [92b] and Halter-Koch [92e].

Lengths of factorizations in other domains were dealt with in Chapman, Geroldinger [97].

For other results concerning factorizations, irreducible integers, and related questions see D.F.Anderson, Pruis [91], Bumby [67], Bumby, Dade [67], Butts, Pall [67], Chapman, Smith [93a], [98], Halter-Koch [93c], Lettl [87], Pall [45].

An abstract approach to factorization problems was presented in Halter-Koch [92b].

EXERCISES

1. Let $n \geq 1$ be an integer. An algebraic number field K satisfies the condition V_n, if any equality of the form $a_1 a_2 = b_1 \cdots b_k$, with a_i, b_j being irreducible integers in K, can hold only if $k \leq n$. Moreover, K satisfies the condition W_n if such an equality with $a_1 = a_2$ implies $k = 2$.

(i) (Czogała [81]) Prove that $h(K) = 3$ holds if and only if K satisfies the condition W_3, but not V_2, and $h(K) = 4$ holds if and only if K satisfies either W_4 or V_3, but does not satisfy W_3.

(ii) (Feng [85]) Prove that K satisfies V_n if and only if $D(H(K)) \leq n$.

2. (Krause [84] If A is a finite Abelian group, then the *cross-number* $k(A)$ of A is defined as the maximal value of the function

$$F(b) = \sum_{a \in b} \frac{1}{o(a)},$$

(where $o(a)$ denotes the order of a) in the set of all irreducible blocks $b \in \mathfrak{B}(A)$.

(i) Prove that if A is a direct sum of cyclic groups of orders $n_1, \ldots, n_s \geq 2$, then

$$k(A) \geq s - \sum_{i=1}^{s} \frac{1}{n_i} + \frac{1}{e},$$

where $e = e(A)$ is the exponent of A, i.e., $e = LCM(n_1, \ldots, n_s)$.

(ii) Prove that if $k(A) = 1$, then A is either cyclic, or its order is a prime power.

(iii) Establish the converse of (ii).

(iv) Show that $H(K)$ is either cyclic, or of a prime-power order if and only if there exists an integer $N \geq 1$ such that the N-th power of every irreducible integer of K is a product of at most N absolutely irreducible elements.

3. (Halter-Koch [84b]). Show that if e is the exponent of $H(K)$, then for every $n = 2, 3, \ldots, e$ one can find non-associated integers $a_0, a_1, \ldots, a_n \in K$ with $a_0^n = a_1 \cdots a_n$.

4. (Halter-Koch [83]). Prove that an irreducible integer $c \in K$ is absolutely irreducible if and only if for every $a, b \in R_K$ the condition $c|ab$ implies either $c|a^2$, or $c|b^2$.

5. Prove that $M(C_3^n) = n$ and $M(C_5^n) = 2n$.

6. Prove that if $h(K) \geq 2$, then for any given positive N almost all integers of K have at least N distinct factorization into irreducibles.

7. Prove that if $h(K) \geq 3$, then almost all integers of K have factorizations into irreducibles of distinct lengths.

8. Prove that if $K/\mathbb{Q}$ is normal and $h(K) \geq 3$, then almost all rational integers have in K factorizations of distinct lengths.

Appendix I

Locally Compact Abelian Groups

1. In this appendix we collect definitions and results from the theory of locally compact Abelian groups used in this book. Several theorems will be quoted without proofs, which can be found e.g. in Hewitt, Ross [63], or Rudin [62].

A *locally compact Abelian group* (LCA) is an Abelian group with a Hausdorff topology in which G is a locally compact topological space. Moreover it is required that the map $G \times G \longrightarrow G$ defined by $[x, y] \mapsto x - y$ is continuous in this topology.

Every such group is a homogeneous space, since for every fixed $a \in G$ the map $x \mapsto ax$ is a homeomorphism. Moreover, to ensure local compactness of G it suffices to have an open neighbourhood of the zero element which has a compact closure.

A continuous homomorphism of G into T, the group of complex numbers with unit absolute value with the usual topology of the circle, is called a *character* of G. The set $\hat{G}$ of characters has a group structure with multiplication given by $(f \cdot g)(x) = f(x)g(x)$ $(f, g \in \hat{G},\ x \in G)$. The family

$$U(\epsilon, X) = \{f \in \hat{G} :\ |f(x) - 1| < \epsilon \text{ for all } x \in X\},$$

where $\epsilon > 0$, and X is a compact subset of G, defines a topology in $\hat{G}$ under which it becomes a locally compact Abelian group, the *group of characters*, or the *dual group* of G.

Every element g of G induces a character on the dual group, namely $g(f) = f(g)$ $(f \in \hat{G})$, and this defines a map $t :\ G \longrightarrow \hat{\hat{G}}$.

Theorem I. (Duality theorem) *The map t is a topological isomorphism of G onto $\hat{\hat{G}}$.*

Theorem II. *The dual group of a discrete group is compact, and the dual group of a compact group is discrete.*

Theorem III. *The dual group of the direct sum $G_1 \oplus G_2$ is isomorphic to $\hat{G}_1 \oplus \hat{G}_2$.*

Theorem IV. *Let $G_1, G_2, \ldots$ be a sequence of compact Abelian groups, and for $i = 2, 3, \ldots$ let $G_i \longrightarrow G_{i-1}$ be a continuous surjective homomorphism. Then the group $G = \liminv G_i$ is compact, and the dual groups $\hat{G}_i$ form in a natural way a direct system of groups, whose limit is topologically isomorphic to $\hat{G}$.*

Proof : The group G is compact, since every projective limit of compact groups is compact. For $i > j$ let a map $f_{ij} : G_i \longrightarrow G_j$ be defined by

$$f_{ij} = f_{j+1} \circ f_{j+2} \circ \cdots \circ f_i.$$

If X_j is a character of G_j, then $X_j \circ f_{ij}$ is a character of G_i, and if we define for $i \geq j$ the map $g_{ij} : \hat{G}_j \longrightarrow \hat{G}_i$ by

$$g_{ij} : X_j \mapsto X_j \circ f_{ij},$$

then $\langle G_i; g_{ij} \rangle$ will be a direct system. Moreover, all maps g_{ij} are injective, hence the direct limit of this system may be identified with the union $\bigcup_i \hat{G}_i$, if we cease to distinguish between X_j and $g_{ij}(X_i)$. No topological questions arise, since by Theorem II all groups involved are discrete. Now, every element of this direct limit defines a character X_i of G_i for i large enough, and if $x = [x_1, x_2, \ldots] \in G$ $(x_i \in G_i)$, then

$$X(x) = X_i(x_i) \quad (i \text{ large enough})$$

defines unambiguously a character of G. Conversely, one sees easily that in this way one obtains every character of G, and it remains to observe that this correspondence preserves multiplication. □

Theorem V. *Let G be a compact Abelian group and*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots$$

let be an infinite sequence of open subgroups of G, having only the unit element in common. If one defines for $j \geq i$ the maps $f_{ij} : G/G_i \longrightarrow G/G_j$ by $f_{ij}(xG_i) = xG_j$, then the inverse limit of the resulting system is topologically isomorphic with G.

Proof : Put $H = \liminv G/G_i$. Since all G_i's are open and G is compact, the quotients G/G_i are finite, hence H is compact. Let $f : G \longrightarrow H$ be given by $f(a) = [aG_i]_i$. This map is obviously continuous, and it is also injective since $f(a) = e$ implies $a \in \bigcap_i G_i = \{e\}$. Thus f is a topological isomorphism of G onto a closed subgroup of H, and it remains to show that $f(G)$ is dense in H. Let $y = [x_i G_i]_i \in H$. For $j \leq i$ we have

$$x_i G_i = x_j G_j H_i = x_j G_i,$$

hence for $y_N = f(x_N)$ we obtain

$$y_N = [x_N G_i]_i = [x_1 G_1, \ldots, x_{N-1} G_{N-1}, x_N G_N, x_N G_{N+1}, \ldots],$$

and so y_N tends to y. □

2. We will also need the concept of *quasicharacters* of a locally compact Abelian group G, i.e., its continuous homomorphisms into $\mathbb{C}^*$, the multiplicative group of complex numbers. In the same way as for characters one introduces group structure and a locally compact topology into the set $\tilde{G}$ of all quasicharacters of G. We prove now some simple facts about quasicharacters, and present a few examples.

Theorem VI. *Let G be a locally compact Abelian group.*

(i) The group $\tilde{G}$ is topologically isomorphic with the direct product of $\hat{G}$ and the group H of positive quasicharacters of G,

(ii) Every bounded quasicharacter is a character,

(iii) If G is compact, or if every element of G is of finite order, then every quasicharacter of G is necessarily a character.

Proof: (i) Only the trivial character is positive, hence $\tilde{G} \cap H = \{e\}$. Moreover, if q is a quasicharacter, then $q(x)/|q(x)|$ is a character, and $|q(x)|$ is a positive quasicharacter, thus $\hat{G}H = \tilde{G}$. The topologies of $\tilde{G}$ and $\hat{G} \times H$ coincide, because each of them is the topology of uniform convergence on compact sets.

(ii) Obvious.

(iii) If G is compact, then every quasicharacter of it is bounded, and we can apply (ii). If every element of G has finite order, then for $x \in G$ and a certain positive integer $n(x)$ we have $x^{n(x)} = e$, thus for every quasicharacter q we have

$$1 = q(x^{n(x)}) = q(x)^{n(x)},$$

whence $|q(x)| = 1$, and q is a character. □

Note also that just as in the case of characters one can prove that the group of quasicharacters of $G_1 \times G_2$ is topologically isomorphic with $\tilde{G}_1 \times \tilde{G}_2$.

3. Now we present some examples. First, let G be the infinite cyclic group with discrete topology. In this case the group $\tilde{G}$ is topologically isomorphic with $\mathbb{C}^*$, the isomorphism given by the map $q \mapsto q(a)$, where a is a fixed generator of G.

Now let G be the additive group R^+ of real numbers with the usual topology. As G is self-dual, it suffices to find its positive quasicharacters, hence to solve the functional equation $q(x + y) = q(x)q(y)$ under the conditions that q is continuous and its values are positive. It is easily seen that with a suitable real α we have $q(x) = e^{\alpha x}$, and so $\tilde{\mathbb{R}}^+$ is topologically isomorphic with $\mathbb{R}^+ \times \mathbb{R}^+$, thus every quasicharacter has the form $q(x) = e^{zx}$ with $z \in \mathbb{C}$.

Similarly one sees that for the additive group $\mathbb{C}^+$ of complex numbers one has $\tilde{\mathbb{C}}^+ \sim \mathbb{C}^+ \times \mathbb{C}^+$, and every quasicharacter has the form $\exp(z_1 \mathrm{Re}\, x + z_2 \mathrm{Im}\, x)$ with complex z_1, z_2.

The last example shows that the analogue of Theorem I does not hold for quasicharacters, since the group of quasicharacters of $\tilde{\mathbb{C}}^+$ equals $(\mathbb{C}^+)^4$.

The next two examples concern multiplicative groups of the real and complex field. First let $G = \mathbb{R}^*$ with the usual topology. Since $\mathbb{R}^* \sim C_2 \times \mathbb{R}^+$, hence $\tilde{\mathbb{R}}^* \sim C_2 \times \mathbb{C}^+$, and every quasicharacter has the form

$$q(x) = (\operatorname{sgn} x)^{\epsilon} |x|^z,$$

where $\epsilon \in \{0, 1\}$ and $z \in \mathbb{C}$.

Finally, the multiplicative group $\mathbb{C}^*$ of complex numbers is isomorphic to $T \times \mathbb{R}^+$, thus $\tilde{\mathbb{C}}^* \sim \tilde{T} \times \tilde{\mathbb{R}}^+ \sim C_\infty \times \mathbb{C}^+$, and every quasicharacter is of the form

$$q(x) = \exp(in \arg x)|x|^z,$$

with $n \in \mathbb{Z}$ and $z \in \mathbb{C}$.

Note that in the last two examples one can write the quasicharacters in a uniform way:

$$q(x) = \left(\frac{x}{|x|}\right)^n |x|^z.$$

4. We will also use the Haar measure and Haar integral in locally compact Abelian groups. By a *Haar measure* on G we understand any Borel measure μ on G which is translation invariant, i.e. for every $x \in G$ and every Borel set $E \subset G$ one has $\mu(E + x) = \mu(E)$, and which is positive on every open and non-void subset of G. In every LCA there is such a measure, and it is essentially unique, i.e., if μ and μ_1 are two Haar measures on G, then the equality $\mu(E) = c\mu_1(E)$ holds for every Borel set $E \subset G$, with a constant c independent of E. It is convenient to choose the Haar measure in a compact group G so that $\mu(G) = 1$, and in a discrete group so that every one-element set has unit measure.

The *Haar integral* is the integral taken with respect to a Haar measure. For a thorough study of its properties see Hewitt, Ross [63].

The linear space of measurable complex-valued functions on G, whose absolute value has a finite Haar integral, will be denoted, as usual, by $L_1(G)$. For $f \in L_1(G)$ one can define its *Fourier transform* by

$$\hat{f}(X) = \int_G f(x)X(-x)d\mu(x), \quad (X \in \hat{G})$$

which is a continuous function on the dual group of G.

In a similar way one defines the *Mellin transform* on G. If f is a complex-valued measurable function on G, and $q \in \tilde{G}$, then the integral

$$\tilde{f}(q) = \int_G f(x)q(x)d\mu(x)$$

may happen to be finite. In this case we speak about the value of the Mellin transform at q.

We present now some examples of the Mellin transform:

(a) $G = C_\infty$ with discrete topology. Here

$$\tilde{f}(q) = \tilde{f}(z) = \sum_{n=-\infty}^{\infty} f(n) z^n,$$

since every quasicharacter corresponds to an element $z \in \mathbb{C}^*$.

(b) $G = \mathbb{R}^+$ with the usual topology. Here quasicharacters correspond to elements of $\mathbb{C}^+$, and we have

$$\tilde{f}(q) = \tilde{f}(z) = \int_{-\infty}^{\infty} f(x) e^{zx} dx = 2\pi i L(f; -z),$$

where $L(f; w)$ is the classical Laplace transform.

(c) $G = \mathbb{C}^+$ with the usual topology. Here

$$\tilde{f}(q) = \tilde{f}(z_1, z_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x + iy) e^{z_1 x + z_2 y} dx dy.$$

(d) $G = \mathbb{R}^*$ with the usual topology. Here the Haar measure $\mu_{\mathbb{R}}$ is defined by

$$\mu_{\mathbb{R}}(A) = \int_A \frac{dx}{|x|},$$

and we obtain

$$\tilde{f}(q) = \tilde{f}(\epsilon, z) = \int_{|x|>0} (\operatorname{sgn} x)^\epsilon |x|^{z-1} f(x) dx.$$

(e) $G = \mathbb{C}^*$ with the usual topology. For the Haar measure $\mu_{\mathbb{C}}$ we may take

$$\mu_{\mathbb{C}}(A) = \int_A \frac{dx dy}{x^2 + y^2},$$

and we obtain

$$\tilde{f}(q) = \tilde{f}(n, z) = \iint \exp(in \arg(x + iy)) |x^2 + y^2|^{z/2-1} f(x + iy) dx dy,$$

the integral being taken over the set of all $(x, y) \neq (0, 0)$.

We shall also use the following result:

Inversion Theorem. *If G is a LCA and μ is its Haar measure, then there exist a unique Haar measure $\hat{\mu}$ on the dual group $\hat{G}$ such that for every continuous and integrable function f on G, whose Fourier transform $\hat{f}$ is also integrable, the following formula holds:*

$$f(x) = \int_{\hat{G}} \hat{f}(X) X(x) d\hat{\mu}(x) = \hat{\hat{f}}(-x).$$

In particular, if G is self-dual, then one can choose the Haar measure so that the inversion formula holds with the same measure on G and $\hat{G}$. In the case of $G = \mathbb{R}^+$ the usual Lebesgue measure will have this property, and for $G = \mathbb{C}^+$ it will be the double of the Lebesgue plane measure, provided we establish the following correspondence between the elements of $\mathbb{C}^+$ and its dual: if $G = \mathbb{R}^+$, then $a \in G \leftrightarrow X_a(t) = \exp(-2\pi i a t)$, and if $G = \mathbb{C}^+$, then $a \in G \leftrightarrow X_a(t) = \exp(-4\pi \mathrm{Re}\,(ax))$. This assertion results immediately from the following easily verifiable equalities:

$$\int_{-\infty}^{\infty} e^{-x^2+2\pi i y x} dx = \sqrt{\pi} e^{-\pi^2 y^2},$$

$$\int_{-\infty}^{\infty} e^{-\pi^2 y^2 - 2\pi i y x} dy = \frac{1}{\sqrt{\pi}} e^{-y^2},$$

$$\iint_{\mathbb{R}^2} e^{-x^2-y^2+4\pi(x x_1 - y y_1)} dx dy = \pi e^{-4\pi^2(x_1^2+y_1)^2},$$

$$2\pi \iint_{\mathbb{R}^2} e^{-4\pi^2(x_1^2+y_1^2)-4\pi(x x_1 - y y_1)} dx_1 dy_1 = e^{-x^2-y^2}.$$

5. We prove now the analogue of Theorem 5.46 for the fields $\mathbb{R}$ and $\mathbb{C}$:

Theorem VII. (J.Tate [50]) *Let K be either the real, or the complex field, let*

$$v(x) = \begin{cases} |x| & \text{if } K = \mathbb{R}, \\ |x|^2 & \text{if } K = \mathbb{C}. \end{cases}$$

Let f be a complex-valued function defined on K, which is continuous and integrable with respect to the Haar measure μ in K^+. Assume, moreover, that its Fourier transform is also integrable, and that for all $t > 0$ the functions $f(x)v(x)^t$ and $\hat{f}(y)v(y)^t$ lie in $L_1(K^*)$. For every quasicharacter $q(x) = X(x)v(x)^s$ of K^* (where $X(x) = (\mathrm{sgn}\, x)^\epsilon$, $\epsilon \in \{0, 1\}$ for K real, and $X(x) = (x/|x|)^n$ with $n \in \mathbb{Z}$ for K complex) define a quasicharacter $\hat{q}$ by $\hat{q}(x) = v(x)/q(x)$. Then for the zeta-function

$$Z(f, q) = \int_{K^*} f(x) q(x) d\mu(x)$$

the functional equation

$$Z(f, q) = \rho(q) Z(\hat{f}, \hat{q})$$

holds for $0 < \mathrm{Re}\, s < 1$, where for $K = \mathbb{R}$ we have

$$\rho(q) = \begin{cases} \pi^{(1-s)/2}\Gamma(s/2)/\pi^{s/2}\Gamma((1-s)/2) & \text{if } \epsilon = 0, \\ \pi^{1-s/2}\Gamma((1+s)/2)/i\pi^{(1+s)/2}\Gamma(1-s/2) & \text{if } \epsilon = 1, \end{cases}$$

and for $K = \mathbb{C}$

$$\rho(q) = (-i)^{|n|} \frac{(2\pi)^{1-s}\Gamma(s + |n|/2)}{(2\pi)^s \Gamma(1 - s + |n|/2)}.$$

Moreover, for a fixed equivalence[1] *class of quasicharacters the zeta-function is a regular function of s in the half-plane* $\operatorname{Re} s > 0$, *and can be continued to a meromorphic function in the plane.*

Proof: We proceed in the same way as in the proof of Theorem 5.46. However, we have to make an appropriate choice of the auxiliary function g, occurring in that proof. If $K = \mathbb{R}$ and $\epsilon = 0$, then we put $g(x) = e^{-\pi x^2}$, in which case we get $\hat{g} = g$, and $Z(g, q) = \pi^{-s/2}\Gamma(s/2)$, thus

$$Z(\hat{g}, \hat{q}) = \pi^{-(1-s)/2}\Gamma((1-s)/2).$$

If $K = \mathbb{R}$ and $\epsilon = 1$, then put $g(x) = xe^{-\pi x^2}$. In this case $\hat{g}(y) = ig(y)$, and to compute the zeta-functions write

$$\begin{aligned} Z(g, q) &= \int_{-\infty}^{0} xe^{-\pi x^2}|x|^{s-1}dx - \int_{0}^{\infty} xe^{-\pi x^2}|x|^{s-1}dx \\ &= 2\int_{0}^{\infty} e^{-\pi x^2}x^s dx = \pi^{-(s+1)/2}\Gamma((s+1)/2), \end{aligned}$$

and similarly

$$Z(\hat{g}, \hat{q}) = i\pi^{-(2-s)/2}\Gamma((2-s)/2).$$

If $K = \mathbb{C}$, then put

$$g(x) = g_n(x) = \begin{cases} \bar{x}^n \exp(-2\pi|x|^2) & \text{if } n \geq 0, \\ x^{-n} \exp(-2\pi|x|^2) & \text{if } n < 0. \end{cases}$$

In this case for $n = 0$ and $\hat{x} = x + iy$ we obtain

$$\begin{aligned} \hat{g}_0(\hat{x}) =& 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp(-2\pi(u^2 + v^2 - 2i(xu - yv)))dudv \\ =& 2\int_{-\infty}^{\infty} \exp(-2\pi(u^2 + v^2 - 2ixu))du \int_{-\infty}^{\infty} \exp(-2\pi v^2 - 4\pi iyv)dv \\ =& \exp(-2\pi(x^2 + y^2)) = g_0(\hat{x}). \end{aligned}$$

For non-zero n we assert that $g_n(x) = i^{|n|}g_{-n}(\hat{x})$. This being true for $n = 0$, let us assume that it holds for a certain $n \geq 0$. Writing this down explicitly, and applying the operator

$$\frac{1}{4\pi i}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right),$$

we immediately obtain the truth of our assertion for $n+1$. Having established this for non-negative n, we obtain it also for negative n with the use of the inversion theorem.

For the zeta-functions one gets now without difficulties the equalities

---

[1] Recall, that two quasicharacters Xv^s and $X_1v^{s'}$ are called equivalent if $X = X_1$.

$$Z(g_n, q) = (2\pi)^{1-s+|n|/2}\Gamma(s + |n|/2),$$

and

$$Z(\hat{g}_n, \hat{q}) = i^{|n|}(2\pi)^{s+|n|/2}\Gamma(1 - 2s + |n|/2).$$

Once this is done, one proceeds in the same way as in the proof of Theorem 5.46, and arrive safely at our assertion. □

6. In this section we state and prove the *Poisson formula*, but only in a special case, needed in Chap. 6. Let G be a locally compact Abelian group, H its discrete subgroup, and assume that the factor group G/H is compact in the quotient topology. The dual group of G/H will be denoted by $\mathfrak{G}$. Note that $\mathfrak{G}$ can be identified with the subgroup of $\hat{G}$, consisting of characters which are trivial on H. Assume, moreover, that there exists an open set $D \subset G$ such that every $g \in G$ can be written uniquely in the form $g = hd$, with $h \in H$, $d \in D$. This assumption allows us to consider the map $f : G/H \longrightarrow D$ defined by $f(A) = x$, where $x \in D$ is a representative of the coset A. This map is continuous, and thus D is compact. If we choose in G a Haar measure m with $m(D) = 1$, then it induces a Haar measure μ in G/H, via $\mu(E) = m(f(E))$, under which G/H acquires the unit measure. Finally, let ν be the Haar measure on H, giving the unit measure to every one-element set. Note that with this choice of measures we have for $f \in L_1(G)$ the equality

$$\int_G f(x)dm(x) = \int_H \int_G f(x + h)dm(x)d\nu(h) = \sum_{h\in H} \int_D f(x + h)dm(x).$$

Under these assumptions we now prove Poisson's formula:

Theorem VIII. *Let f be a continuous function in $L_1(G)$, and assume that*

(i) the series $\sum_{h\in H} f(x + h)$ converges uniformly for $x \in D$,

and

(ii) the series $\sum_{y\in\mathfrak{G}} |\hat{f}(y)|$ converges.

Then we have

$$\sum_{h\in H} f(h) = \sum_{y\in\mathfrak{G}} \hat{f}(y).$$

Proof : Put

$$g(x) = \begin{cases} \sum_{h\in H} & \text{if } x \in D, \\ 0 & \text{otherwise,} \end{cases}$$

and let $\chi \in \mathfrak{G}$. We may assume that χ is a character of G, trivializing on H. Then

$$\hat{g}(\chi) = \int_D \sum_{h\in H} f(x+h)\chi(-x)dm(x) = \sum_{h\in H}\int_D f(x+h)\chi(-x)dm(x)$$
$$= \sum_{h\in H}\int_{h+D} f(x)\chi(h-x)dm(x) = \sum_{h\in H}\chi(h)\int_{h+D} f(x)\chi(-x)dm(x)$$
$$= \sum_{h\in H}\int_{h+D} f(x)\chi(-x)dm(x) = \int_G f(x)\chi(-x)dm(x) = \hat{f}(\chi).$$

We can regard g as a function on G/H, owing to the biunique correspondence between G/H and D. One sees easily that the Fourier transform of this function coincides with $\hat{g}$, and by the inversion formula we get

$$g(x) = \sum_{\chi\in\mathfrak{G}} \hat{g}(\chi)\chi(x) \quad \text{for } x \in D,$$

hence

$$\sum_{h\in H} f(x+h) = \sum_{\chi\in\mathfrak{G}} \hat{f}(\chi)\chi(x),$$

and putting $x = 0$ in the last equality we obtain our assertion. □

7. In this subsection we develop the main properties of the *restricted direct product* of topological Abelian groups, which are needed in Chap. 6. We start with the definition:

Let $\{G_v\}_v$ be a family of locally compact Abelian groups, indexed by elements v of a set V, and assume that for almost every v (i.e. for all except finitely many) a compact and open subgroup H_v of G_v is selected. The restricted product G of the G_v's with respect to the H_v's is the subgroup of the product $\prod_v G_v$, consisting of all elements $\langle g_v\rangle_v$ such that for almost all v one has $g_v \in H_v$. In G we define a topology by taking for the fundamental system of neighbourhoods of the unity the system of all such neighbourhoods in the product topology in the groups

$$G_S = \prod_{v\in S} G_v \times \prod_{v\notin S} H_v,$$

where S is an arbitrarily fixed finite set of indices containing every index v for which H_v is left undefined. One sees without difficulty that this topology does not depend on the particular choice of S, and that all groups G_v are open in G. It is also easy to see that the family $\{\prod_v U_v\}$, where U_v is a neighbourhood of unity in G_v, and for almost all v's we have $U_v = H_v$, can also serve as a fundamental system of neighbourhoods of unity in G.

Lemma 1. *The restricted product G is a LCA.*

Proof : The continuity of the operations is immediate, and the local compactness follows from the observation that for finite S the group G_S is locally compact, and open in G. □

The following theorem describes characters and quasicharacters in restricted products:

Theorem IX. *(i) The character group $\hat{G}$ is topologically isomorphic with the restricted product of the groups $\hat{G}_v$ with respect to the subgroups $A_v \subset \hat{G}_v$, annihilating H_v (i.e. consisting of characters trivial on H_v). Moreover, for $\chi \in \hat{G}$ we have*

$$\chi(\langle g_v \rangle) = \prod_v \chi_v(g_v),$$

where χ_v is the restriction of χ to G_v, considered as a subgroup of G via the embedding $g_v \mapsto (h_w)_{w \in V} \in G$, with

$$h_w = \begin{cases} g_v & \text{if } w = v, \\ e_w & \text{otherwise,} \end{cases}$$

where e_w is the unit element of the group G_w.

(ii) The same assertion holds for the group of quasicharacters. However, this time the isomorphism is only algebraical, not necessarily topological.

Proof : Let q be a quasicharacter of G, and let q_v be its restriction to G_v. We show that for almost all v's we have $q_v(H_v) = 1$. In fact, if U is a neighbourhood of unity in $\mathbb{C}^*$, not containing nontrivial subgroups, and $O = \prod_v O_v$ is a neighbourhood of unity in G, satisfying $q(O) \subset U$, then q is trivial on every subgroup of O. However, for almost all v's we have $O_v = H_v \subset O$, thus q is trivial on any such H_v. Let S be the set of those $v \in V$ for which either H_v is undefined, or q is non-trivial on H_v. Let also $g = \langle g_v \rangle \in G$ be arbitrary, and put $T = \{v \notin S : \ g_v \notin H_v\}$ and $S_1 = \{v \notin S \cup T : \ H_v = O_v\}$. Write

$$g = \prod_{v \in S} g_v \prod_{v \in T} g_v \prod_{v \in S_1} g_v \cdot g_0,$$

with $g_0 \in \prod_v O_v$. Then

$$q(g) = \prod_{v \in S \cup T \cup S_1} q(g_v) q(g_0) = \prod_{v \in S \cup T \cup S_1} q(g_v) = \prod_v q(g_v),$$

because for v outside $S \cup T \cup S_1$ we have $q(g_v) = 1$.

Now note that if for every v we have a quasicharacter q_v of G_v, and for almost all v this quasicharacter is trivial on H_v, then the formula $q(\langle x_v \rangle_v) = \prod_v q_v(x_v)$ defines a quasicharacter of G. The multiplicative property of q is evident, and to obtain its continuity denote by S the set of indices v, for which q_v is non-trivial on H_v, and let $N = \#S$. For every neighbourhood U of 1 in the complex plane choose a neighbourhood U_1 with $U_1^N \subset U$. If now the open sets $U_v \subset G_v$ are chosen so that $X_v(U_v) \subset U_1$ holds for $v \in S$, and $U_v = H_v$ holds for $v \notin S$, then the quasicharacter q maps the product $\prod_v U_v$ into U, and so is continuous.

Consider now the map

$$\varphi : \langle q_v \rangle_v \mapsto \prod_v q_v$$

of the restricted product A of the groups $\tilde{G}_v$ with respect to their subgroups annihilating H_v into $\tilde{G}$. It is obviously injective, and the preceding argument shows that it is also surjective. This proves part (ii) of the theorem.

Observe now that φ maps A onto the group $\hat{G}$. Therefore these two groups are algebraically isomorphic. We prove now that φ is a topological isomorphism.

A set $C \subset G$ has a compact closure if and only if it lies in $\prod_v C_v$, where $C_v \subset G_v$ is compact, and for almost all v we have $C_v = H_v$. Indeed, every such set has a compact closure, and on the other hand, if $\overline{C}$ is compact, then for a certain finite $S \subset V$ we have $C \subset G_S$, because $\overline{C} \subset G = \bigcup_S G_S$, and so a finite system of open subgroups G_S covers $\overline{S}$. It remains to observe that a finite union of sets G_S also has this form.

Let U be a neighbourhood of unity in $\hat{G}$, having the form

$$U = \{\chi : \ |\chi(t) - 1| < \epsilon \quad \text{for } t \in \prod_v C_v\},$$

with $0 < \epsilon < 1/2$ and finite $S = \{v : \ C_v \neq H_v\}$. If $X \in U$, then for $t_v \in C$ we have $|\chi_v(t_v) - 1| < \epsilon$, and for v outside S we have $\chi_v(t_v) = 1$, because then $C_v = H_v$ is a group, and $\chi_v(H_v)$ lies in the disc $\{z : \ |z - 1| < 1/2\}$.

If

$$U_v = \{q \in \tilde{G}_v : \ |q(t) - 1| < \epsilon \quad \text{for } t \in C_v\},$$

then $\chi \in U$ implies $\chi_v \in U_v$ for v in S, and $\chi_v(H_v) = 1$ for $v \notin S$. Conversely, if χ_v satisfies the two last conditions, then for t in $\prod_{v \in S} C_v \times \prod_{v \notin S} H_v$ we have $|\chi(t) - 1| < \epsilon'$ for suitable ϵ', depending on ϵ. □

8. Now we turn to the Haar measure in a group G, which is the restricted product of G_v's with respect to H_v's. We retain all notation from the preceding subsection. Choose in every G_v a Haar measure μ_v, giving the unit measure to the groups H_v in the case, when they are defined. It is also possible to allow finitely many exception to this condition. For every finite $S \subset V$ denote by μ^S the product measure in the compact group $\prod_{v \notin S} H_v$. Then

$$\mu_S = \prod_{v \in S} \mu_v \times \mu^S$$

is a Haar measure in the group G_S.

If f is a continuous function with compact support A on G, then for suitable S we have $A \subset G_S$, and so the linear functional

$$F(f) = \int_{G_S} f(x) d\mu_S(x)$$

is well defined and independent of the choice of S. This functional induces, in a well-known way, an invariant integral on G. Thus there exists a Haar measure μ on G for which

$$F(f) = \int_G f(x)d\mu(x).$$

This measure depends on the choice of Haar measures in those groups G_v, for which H_v is not defined. However, in all our applications there will be a standard choice for those measures. The next two lemmas are useful for performing effective integration on G, and for finding Fourier transforms:

Lemma 2. *Assume that for every $v \in V$ a complex-valued, continuous and integrable function f_v on G_v is given, whose restriction to H_v equals 1 for almost all v's. Let f be the function on G defined by*

$$f(\langle x_v \rangle) = \prod_v f_v(x_v).$$

Then f is continuous, and for every finite set $S \subset V$ containing all v's for which either H_v is not defined, or f_v is non-trivial on H_v, we have

$$\int_{G_S} f(x)d\mu(x) = \prod_{v \in S} \int_{G_v} f_v(x_v)d\mu_v(x).$$

Proof : The continuity of f results from the observation that the groups G_S are open and cover G, and on each of them f is continuous. The asserted equality is a consequence of

$$\int_{G_S} f(x)d\mu(x) = \int_{G_S} f(x)d\mu_S(x),$$

and the definition of $d\mu_S(x)$. □

Corollary. *Under the assumptions of the lemma, if*

$$\sup_S \prod_{v \in S} \int_{G_v} |f_v(x_v)|d\mu_v(x) < \infty,$$

then f is integrable on G, and

$$\int_G f(x)d\mu(x) = \prod_v \int_{G_v} f_v(x_v)d\mu_v(x).$$ □

Denote by h_v the characteristic function of H_v for all v, for which H_v is defined. Moreover, let H_v^* be the subgroup of $\hat{G}_v$, annihilating H_v.

Lemma 3. *(i) The Fourier transform of h_v equals the characteristic function of H_v^*.*

(ii) For every $v \in V$ let f_v be a complex-valued, continuous and integrable function on G_v. Assume that for almost all v, one has $f_v = h_v$.

If $f = \prod_v f_v$ is the induced function on G, then its Fourier transform $\hat{f}$ satisfies

$$\hat{f}(\chi) = \prod_v \hat{f}_v(\chi_v),$$

where $\chi = \prod_v \chi_v$ is a character of G in the form given by Theorem IX.

Proof : (i) We have

$$\begin{aligned}\hat{h}_v(\chi_v) &= \int_{G_v} h_v(x)\chi_v(x^{-1})d\mu_v(x) = \int_{H_v} \chi_v(x^{-1})d\mu_v(x) \\ &= \begin{cases} \int_{H_v} d\mu_v(x) = 1 & \text{if } \chi_v \text{ is trivial on } H_v, \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

thus $\hat{h}_v$ is equal to the characteristic function of H_v^*, as asserted.

(ii) It follows from (i) that for almost all v for any character $\chi = \prod_v \chi_v$ we have $\hat{h}_v(\chi_v) = 1$. Moreover, for almost all v we have

$$\int_{G_v} |f_v(x_v)\chi_v(x_v^{-1})|d\mu_v(x) = 1,$$

and so it is possible to apply the corollary to the preceding lemma, yielding

$$\hat{f}(\chi) = \int_G f(x)\chi(x^{-1})d\mu(x) = \prod_v \int_{G_v} f_v(x_v)\chi_v(x_v^{-1})d\mu_v(x) = \prod_v \hat{f}_v(\chi_v).\square$$

The next lemma describes the Haar measure in the character group $\hat{G}$, dual to the Haar measure in G used above. Recall, that one says that the Haar measure $\hat{\mu}$ on $\hat{G}$ is dual to the Haar measure μ on G if the inversion theorem, as stated above, holds for them.

Lemma 4. *For every v let $\hat{\mu}_v$ be the Haar measure on $\hat{G}_v$, dual to the measure μ_v. Then the group H_v^* has unit measure, and the measure $\hat{\mu}$ defined in $\hat{G}$, using the measures $\hat{\mu}_v$ in the same way, as μ was defined with the use of μ_v, is dual to μ.*

Proof. We have

$$h_v(y) = h_v(y^{-1}) = \int_{\hat{G}_v} \hat{h}_v(\hat{x}_v)y(\hat{x}_v^{-1})d\hat{\mu}_v,$$

and

$$h_v(y) = \int_{H_v^*} \overline{\hat{x}_v(y)} d\hat{\mu}_v(x).$$

Putting y equal to the unit element of G, we obtain

$$\int_{H_v^*} d\hat{\mu}_v(x) = 1.$$

Therefore we can apply the process of constructing the Haar measure in $\hat{G}$. The check that the resulting measure is dual to μ does not present any difficulties. □

Corollary. *If f satisfies the conditions of Lemma 3, and, moreover, for all v the Fourier transform of f_v is integrable, then the Fourier transform of f is also integrable.*

Proof : If we put $S_0 = \{v : f_v \neq h_v\}$, then by Lemma 3 (ii) we get

$$\hat{f}(\hat{x}) = \prod_{v \in S_0} \hat{f}_v(\hat{x}_v) \prod_{v \notin S_0} \hat{h}_v(x_v).$$

Lemma 4 and Lemma 3 (i) imply now that for v outside S_0 we have

$$\int_{\hat{G}_v} |\hat{h}_v| d\hat{\mu}_v = 1,$$

and therefore

$$\sup_S \prod_{v \in S} \int_{\hat{G}_v} |\hat{f}_v(\hat{x}_v)| d\hat{\mu}_v \leq \prod_{v \in S_0} \int_{\hat{G}_v} |\hat{f}_v(\hat{x}_v)| d\hat{\mu}_v \leq \infty.$$

It remains to apply Lemma 3 (ii). □

Appendix II

Function Theory

1. We collect here certain results of the theory of complex functions, used in this book. The proofs are omitted.

A series of the form

$$\sum_{n=1}^{\infty} a_n n^{-s}, \tag{1}$$

where a_n are complex coefficients, and $s = \sigma + it$ is a complex variable, is called a *Dirichlet series*.

Proposition 1. *If the series (1) converges at s_0, then it converges also in the open half-plane $\sigma > 1 + \operatorname{Re} s_0$, the convergence being uniform in every angle $\arg(s - s_0) \leq c < \pi/2$. Thus (1) defines a function regular in the half-plane $\sigma > \operatorname{Re} s_0$. If at s_1 the convergence is absolute, then (1) converges absolutely and uniformly in the half-plane $\sigma \geq \operatorname{Re} s_1$.*

This proposition allows us to speak about the half-planes of convergence and absolute convergence of (1).

We are mainly interested in the asymptotic behaviour of the coefficient sum $S(x) = \sum_{a_n \leq x}$ of (1). A very general result regarding this question is the *theorem of Delange-Ikehara*[2], of which the following theorem is a special case:

Theorem I. *Assume that the coefficients of the series (1) are real and non-negative, and that it converges in the half-plane $\sigma > 1$, defining there a regular function $f(s)$. Assume, moreover, that in the same half-plane one can write*

$$f(s) = \sum_{j=0}^{q} g_j(s) \log^{b_j}\left(\frac{1}{s-1}\right)(s-1)^{-\alpha_j} + g(s),$$

where the functions $g, g_0, \ldots, g_q$ are regular in the closed half-plane $\sigma \geq 1$, the b_j-s are non-negative rational integers, α_0 is a positive real number, $\alpha_1, \ldots, \alpha_q$ are complex numbers with $\operatorname{Re} \alpha_j < \alpha_0$, and $g_0(1) \neq 0$.

[2] See Delange [54], Narkiewicz [83,Chap. III].

Then for the summatory function $S(x) = \sum_{n \le x} a_n$ *we have, for* x *tending to infinity,*

$$S(x) = \left(\frac{g_0(1)}{\Gamma(\alpha_0)} + o(1) \right) x \log^{\alpha_0 - 1} x (\log \log x)^{b_0}.$$

If f *satisfies the same assumptions, except that* $\alpha_0 = 0$ *and* $b_0 \ge 1$, *then*

$$S(x) = (b_0 g_0(1) + o(1)) x \frac{(\log \log x)^{b_0 - 1}}{\log x}.$$

Note that in Delange's paper the α_j's are assumed to be real, however this assumption is not used in the proof.

2. We need also a result of Landau. For its proof see e.g. Narkiewicz [83, Th. 3.5] or Prachar [57].

Theorem II. *If* $\sigma > C$ *defines the half-plane of convergence of a series (1) with non-negative coefficients, then the sum of this series has a singularity at* $s = C$.

We also include for reference two results from function theory not connected with Dirichlet series. Their proofs can be found in Prachar [57]. Put $D(s_0; r) = \{s : |s - s_0| \le r\}$.

Theorem III. *Assume that* $f(s)$ *is regular in the disc* $D(s_0; r)$, *and does not vanish in the set*

$$\{s : |s - s_0| \le r/2, \quad \operatorname{Re}(s - s_0) > 0\}.$$

Assume, moreover, that it satisfies

$$\left| \frac{f(s)}{f(s_0)} \right| < M$$

in $D(s_0; r)$. *If* z *is a zero of* f *of order* h, *satisfying* $|z - s_0| \le r/2$, *and* $\operatorname{Re}(z - s_0) < 0$, *then one has the following inequalities:*

$$(i) \quad \operatorname{Re} \left(\frac{f'(s_0)}{f(s_0)} \right) \ge -\frac{4 \log M}{r},$$

and

$$(ii) \quad \operatorname{Re} \left(\frac{f'(s_0)}{f(s_0)} \right) \ge -\frac{4 \log M}{r} + \operatorname{Re} \left(\frac{h}{s_0 - z} \right).$$

Theorem IV. *If* f *is regular in the disc* $D(s_0; R)$, *and* $0 < r < R$, *then for* $s \in D(s_0; r)$ *we have*

$$|f(s)| \le \frac{2|f(s_0)|R}{R - r} + \frac{2r}{R - r} \max_{s \in D(s_0; R)} \operatorname{Re} f(s).$$

Appendix III

Baker's Method

In the proof of Theorem 8.29 the use is made of a result of A.Baker and G.Wüstholz [93], giving a lower bound for linear forms in logarithms. To state it we denote by $H(a)$ the height of an algebraic number a, defined as the maximal absolute value of the coefficients of the minimal polynomial of a over $\mathbb{Q}$.

Theorem. *Let $a_1, a_2, \ldots, a_n$ be non-zero algebraic numbers, and let*

$$L(X_1, X_2, \ldots, X_n) = X_1 \log a_1 + \cdots + X_n \log a_n.$$

Assume that the numbers $A_1, \ldots, A_n$ satisfy $A_j \geq e$, and $H(a_j) \leq A_j$ for $j = 1, 2, \ldots, n$. If $M \geq e$, and $x_1, \ldots, x_n$ are rational integers, satisfying $|x_j| \leq M$ $(j = 1, \ldots, n)$, then either $L(x_1, \ldots, x_n) = 0$, or

$$\log |L(x_1, \ldots, x_n)| > -(16dn)^{2n+4} \log M \prod_{j=1}^{n} \log A_j,$$

where d is the degree of the extension $\mathbb{Q}(a_1, a_2 \ldots, a_n)/\mathbb{Q}$.

Problems

In the first edition a list of 35 open problems was presented, and in the second edition 14 problems were added. In the meantime certain of them have been solved either completely (they are marked by an asterisk), or partially. Here we reproduce this list, and add certain other problems.

1. (Lehmer [33a]) Prove that for every $\epsilon > 0$ one can find an algebraic integer a, not a root of unity, with

$$M(a) = \prod \max(1, |a^{(i)}|) < 1 + \epsilon,$$

where the product runs over all conjugates $a^{(i)}$ of a.

The answer is negative in the case, when the minimal polynomial P of a is not reciprocal, i.e., $P(X) \neq X^n P(1/X)$, with $n = \deg P$ (Breusch [51], Smyth [71]). Now it is rather believed that the answer is negative. See Chap.2 for comments.

2*. (Robinson [62]) Show that if $b - a > 4$, then the interval $[a, b]$ contains a full system of conjugates of an integer of degree n, provided n is sufficiently large.

Solved by Ennola [75a].

3. (Samet [53]) Let U be the set of all non-real integers, whose all conjugates except two lie in the closed unit disc, and there are some on its circumference, Determine the closure of U.

4. (Robinson [69]) Determine all circles with irrational center which contain infinitely many full systems of conjugates of algebraic integers.

Circles of this type with rational centers have been described in Robinson [69]. Circles with totally real centers were described in Ennola [73a], and circles with centers of degree 3 or 4 in Ennola, Smyth [74]. All algebraic integers whose conjugates lie on a circle were described in Ennola, Smyth [76].

5. Determine all numbers which are discriminants of finite extensions of $\mathbb{Q}$.

For Abelian extensions of $\mathbb{Q}$ with a given Galois group the answer is given by the conductor-discriminant formula. In the general case nothing seems to be known apart of Stickelberger's theorem.

6. Find a necessary and sufficient condition for a field to have index 1.

It follows from Uchida [77b] that this happens if and only if the field has an integral generator, whose minimal polynomial does not lie in the square of a maximal ideal in $\mathbb{Z}[X]$. An effective procedure to check whether a given field has index 1 was given by Győry [73].

7. Let $N_k(x)$ denote the number of non-isomorphic fields of degree k whose discriminants do not exceed x in absolute value. Prove the existence of a positive limit $\lim_{x\to\infty} N_k(x)/x$.

For $k = 2$ this is trivial, and for $k = 3$ this has been proved in Davenport, Heilbronn [69]. Lower and upper bounds for $N_4(x)$ have been obtained in Baily [80]. Upper bounds in the general case were given in W.M.Schmidt [95].

8. Find a necessary and sufficient condition for the existence of a normal integral basis in a normal extension.

9. Can one determine reasonable classes of extensions $K/\mathbb{Q}$ for which tame ramification is necessary and sufficient for the existence of a normal basis.

There was an enormous progress on the two last questions. We refer the reader to the book of Fröhlich [83a] on that subject and to the literature quoted in Chap.4.

10. Describe fields K (not necessarily algebraic over $\mathbb{Q}$) having the property that every polynomial $P \in K[X]$ for which there exists an infinite set $X \subset K$ with $P(X) = X$ must be linear.

Algebraic number fields have this property (Narkiewicz [62]), and, more generally, all finitely generated extensions of a prime field (Liardet [70], Lewis [72]). See also Kubota, Liardet [76], Liardet [71], [72], [75].

11. Assume that K has the property indicated in the preceding problem. Prove that if the rational function $f \in K(X)$ maps an infinite subset of K onto itself, then $f(X) = (aX + b)/(cX + d)$.

This is known to be true for a large class of fields (Liardet [70]).

12. Let G be a finite Abelian group. Show that there is an algebraic number field with $H(K) \sim G$. The same problem may be also stated for the group $H^*(K)$.

13. Give a simple criterion for the existence of a unit with negative norm in a real quadratic field.

A rather quick algorithm for testing this was presented in Lagarias [80a].

14. Characterize real fields with a system of totally positive fundamental units.

This is equivalent to $h^*(K) = 2^{r_1-1}h(K)$. See Armitage, Fröhlich [67], where this possibility is ruled out for a large class of fields.

15. Characterize fields with a system of real fundamental units.

16. Give a convenient necessary and sufficient condition for a normal field to have a conjugated system of fundamental units.

17. In which fields has the group $U^+(K)$ a conjugated system of generators?

Fields with cyclic Galois group of 3 and 5 elements have this property. This was proved by Hasse [48a], and Morikawa [68], respectively.

18. (Jacobson [64]) In which fields is every integer a sum of distinct units?

There are only two such quadratic fields (with $d(K) = 5, 8$) (Jacobson [64], Śliwa [74]), but infinitely many cubic and quartic fields (Belcher [74], [75]).

19*. Prove that only a finite number of units in a given field can have the same discriminant.

This was proved in Birch, Merriman [72] and Győry [73[, [83]. Győry's proof is effective.

20. (Heilbronn [50]) Prove the existence of infinitely many Euclidean cubic fields.

21. (Gauss) Show that infinitely many real quadratic fields have class-number 1.

For an heuristical approach see Takhtayan, Vinogradov [82].

22. Give an explicit formula for the highest power of a given prime which divides the index of a field K.

For unramified primes this problem was solved in Śliwa [82a]. See also Del Corso, Dvornicich [02], Gaál, Pethő, Pohst [91], Nakahara [83], Nart [85].

23. (Shafarevich [63a]) Prove that for real quadratic fields with a prime discriminant the rank of $H(K)$ is bounded.

24. (*Leopoldt's Conjecture*, Leopoldt [62]) Find the rank of the p-adic regulator matrix.

In fact Leopoldt conjectured that this rank equals $r_1 + r_2 - 1$. This is true for all Abelian fields, and also in certain other cases. See G.Gras [03,Chap.3], Washington [82,Chap.5].

25. Determine Dedekind domains for which the class of the different of an extension is always a square.

Cf. Fröhlich, Serre, Tate [62].

26. (Artin) Prove that if $K \subset L$, then $\zeta_L(s)/\zeta_K(s)$ is entire.

This holds if the extension L/K is normal (Aramata [31], [33], Brauer [47a]). See also the literature quoted in Chap.7.

27*. Prove the analogue of Proposition 7.19 for non-normal extensions.

This has been done by Odoni [75a] (cf. Odoni [73b], [75b]).

28. Determine the structure of R_L as an $R_K[G]$-module for a given normal extension L/K with Galois group G.

This problem is closely related to problems 8 and 9, and we refer the reader to the literature mentioned there.

29*. Characterize Dedekind domains in which all factorizations into irreducibles of a given element have the same length.

This has been done by Skula [76] (cf. Zaks [76], [80]). For analogues in more general rings see the survey given in Chapman, Coykendall [00].

30. (Davenport) Evaluate Davenport's constant $D(G)$ for finite Abelian groups G.

Cf. the literature quoted in Chap.9.

31*. (Turán) Let $f(n)$ denote the number of distinct factorizations of a given natural number n into irreducibles in an algebraic number field K with $h(K) \neq 1$. Prove that f cannot have a non-decreasing normal order.

Solved by Rosiński and Śliwa [76].

32*. Characterize arithmetically fields with a given class-number $\neq 1, 2$.

This has been done by Kaczorowski [84] and Rush [83]. See Theorem 9.2.

33. Prove that there are only finitely many totally imaginary fields of a given degree and class-number one.

34*. Prove that for any positive integer N there are infinitely many fields of given degree and signature with class-number divisible by N.

This was established for not totally real fields by Azuhata, Ichimura [84], and by Nakano [84] in the remaining case.

35. Give an elementary proof of Dirichlet's class-number formulas.

For imaginary quadratic fields this has been done by Orde [78].

36. (H.C.Williams [81a]) Prove that the length of the period of the continued fraction for $\sqrt{D}$ is $O(\sqrt{D}\log\log D)$.

37. (Browkin, Schinzel) Let K be an algebraic number field. Prove that if there exists an infinite sequence of integers of K, such that for every ideal I the first $N(I)$ terms of this sequence are distinct mod I, then K is the field of rational numbers.

For partial results see Latham [73], Wańtuła [74], Wasén [74], [76], [77].

38. (Boyd [77]) Is the union of the sets of Pisot numbers and Salem numbers closed?

39. (Lenstra [77a]) Evaluate $L(K)$,the Lenstra constant of the field K, defined as the cardinality of the largest set A of integers of K, having the property that for all $a \neq b$ in A the difference $a - b$ is a unit.

40. Characterize fields K in which every totally positive unit is a square.

Cf. Armitage, Fröhlich[67], Garbanati [76], Hasse [52a], Hughes, Mollin [83].

41. For a finite group G characterize $\mathbb{Z}[G]$-modules, which are isomorphic to $U(K)/E(K)$ for suitable normal extensions $K/\mathbb{Q}$ with Galois group G.

See the comments in Chap.3.

42. (Newman [74a]) Which rational integers are sums of two units from the p-th cyclotomic field?

43. (Newman [74a,b], [90]) For a given field K and $\alpha \in R_K$ denote by $N(K,\alpha)$ the maximal number k with the property that there exists a unit $u \in R_K$ such that $u+\alpha, u+2\alpha, \ldots, u+(k-1)\alpha$ are all units.

(a) Determine $N(K,\alpha)$.

The inequality $N(K,\alpha) \leq r_1(K) + r_2(K)$ has been established by K.Győry [79b].

(b) Prove that $N(\mathbb{Q}(\zeta_p),1) = 4$.

This is true for $5 \leq p \leq 37$ and for $p = 47, 73$ ((Newman [90]).

44* (Jehne [77b]) Prove that the only one-element Kronecker class consists of the base field.

A counterexample has been constructed by Saxl [88]. Cf.Lochter [94b].

45*. (Perlis [78]) Do arithmetically equivalent fields have the same class-number?

The answer is negative (de Smit, Perlis [94]).

46. (Baker, Schinzel [71]) Prove that in an imaginary quadratic field of discriminant d every genus contains an ideal of norm $O(|d|^{\epsilon})$ for every $\epsilon > 0$.

The best known bound is $O(|d|^{c})$ for every $c > 1/4$ (Heath-Brown [79]).

47. Obtain analogues of the Frobenius-Rabinowitsch theorem for other values of the class-number and other classes of fields.

Much work has been done on this question. See the book of Mollin [96d] on the quadratic case, as well as the literature quoted in Chap.8.

48. Evaluate the constants $a_1(A)$ and $M(A)$, associated with finite Abelian groups A.

49. (Chowla, Kessler, Livingston [77]). Let $p \equiv 1 \pmod 4$ be a prime. Prove that if for all $x = 1, 2, \ldots, (p-1)/2$ one has

$$\sum_{n=1}^{x} \left(\frac{n}{p}\right) \geq 0,$$

then $p = 5$, 13 or 37.

This has been checked for $p \leq 43\,000$.

Problems added in the third edition:

50. (Sprindzhuk [73], [82]) Let $\epsilon > 0$ be given. Prove that every algebraic number field K of degree n has an extension L/K with

$$[L : K] \leq A, \quad R(L) < B(\epsilon)|d(K)|^{\epsilon},$$

where A depends only on n, and B depends only on n and ϵ.

This is a rather strong conjecture. It implies that for all fields of a fixed degree one has $h(K) \gg |d(K)|^{1/2-\epsilon}$ for every $\epsilon > 0$.

51. (Gordon. This problem has been often attributed to Erdős) Can one walk from the origin to infinity, using steps of bounded length, and the Gaussian primes as the stepping stones?

Jordan, Rabung [70] proved that steps must be $> \sqrt{10}$ and Gethner, Wagon, Wick [98] improved this to $> \sqrt{26}$. Cf. Gethner, Stark [97], Haugland [95].

52. (V.K.Murty [00]) Let L/K be a normal extension, and C a conjugacy class in $Gal(L/K)$. Let $\Pi_C(x, L/K)$ be the number of unramified prime ideals of first degree of norm $\leq x$, whose Frobenius symbol lies in C, and let $p(L/K)$ be the smallest value of x with $\Pi_C(x, L/K) > 0$ for all C. Prove

$$p(L/K) \ll \log^c d(L),$$

with an absolute constant c.

This is true in case when K is the rational field, and L is cyclotomic.

53. Let K be a totally real field, and let A be the set of all totally positive elements of R_K, A number $a \in A$ is said to be indecomposable, if it is not a sum of two elements of A. Determine the maximal norm $c(K)$ of an indecomposable element of A.

For quadratic K this has been done in Dress, Scharlau [82], and a bound for $c(K)$ in the general case was obtained in Brunotte [83].

54. In which fields does every integral basis contain a field generator?

For partial results see de Smit [95].

55. Let K be an algebraic number field, which has infinitely many units. Prove the existence of infinitely many prime ideals $\mathfrak{p}$ in R_K such that every non-zero residue class mod $\mathfrak{p}$ contains units.

This follows from *GRH* (Lenstra [77b]). Unconditionally this has been proved for all Abelian totally real fields of degree ≥ 4 and for totally real quadratic and cubic fields with at most three exceptions (Narkiewicz [88]).

56. (*Artin's Conjecture for number fields*) Prove that if $a \in R_K$ is neither zero, nor a unit, nor a square of an integer in R_K, then there are infinitely many prime ideals in R_K for which a is a primitive root.

This is true under *GRH* (Lenstra [77b]). For partial unconditional results see Narkiewicz [87]). Cf. Hinz [86].

57. (Bremner [88]) Let $K = \mathbb{Q}(\zeta_p)$. Prove that if $\alpha \in R_K$ and $R_K = \mathbb{Z}[\alpha]$, then up to equivalence and conjugation one has either $\alpha = \zeta_p$ or $\alpha = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{(p-1)/2}$.

This is true for $p = 7$ (Bremner [88]).

58. (Stevenhagen [95]) Let $F(x)$ denote the number of real quadratic fields K with $d(K) \leq x$, in which there exists units with negative norm. Prove that with a certain $c > 0$ one has $F(x) = (c + o(1))x/\sqrt{\log x}$

59. (Tollis [97]) Prove that for every n there exists a constant $C(n)$ such that for every field K of degree n the function $\zeta_K(s)$ has a root ρ, satisfying $\operatorname{Im} \rho \leq C(n)/\log|d(K)|$.

The bound $\ll C(n)/\log\log\log(|d(K)|)$ was obtained in Neugebauer [88], and *GRH* permits to eliminate one of the logarithms (Omar [00]).

60. (Morton, Silverman [94]) Let K be an algebraic number field of degree n, and let $f \in K[X]$ be of degree ≥ 2. Assume that f has a cycle of length k in K, i.e., there exist distinct elements $x_1, \ldots, x_k$ in K such that $f(x_k) = x_1$, and $f(x_i) = x_{i+1}$ holds for $i = 1, 2, \ldots, k-1$. Prove that k does not exceed a bound $B(d, n)$, depending only on d and n, but not on K or f.

This is open already in the simplest case $n = 1$, $d = 2$. It is known only that quadratic polynomials with rational coefficients cannot have cycles of length 4 (Morton [92,II]), or 5 (Flynn, Poonen, Schaefer [97]).

References

Abrashkin V.A. [74]: Determination of imaginary quadratic fields with even discriminant and class-number two by Heegner's method, Mat. Zametki, **15**, 1974, 241–246. (Russian)

Acciaro,V.,Fieker,C. [00]: Finding normal bases of cyclic number fields of prime degree, J. Symbolic Comp., **30**, 2000, 129–136.

Adachi,N. [73]: Generalization of Kummer's criterion for divisibility of class numbers, J. Number Theory, **5**, 1973, 253–265.

Adachi,N. [85]: Dedekind domains which are not obtainable as finite integral extensions of PID, Proc. Japan Acad. Sci., **61**, 1985, 281–282.

Agou,S. [71]: Remarques sur la détermination des nombres premiers décomposés dans les corps de nombres du 3ème degré, Publ. Dept. Math. Lyon, **8**, 1971, no.2, 93–100.

Ahern,P.R. [64]: The asymptotic distribution of prime ideals in ideal classes, Indag. Math., **26**, 1964, 10–14.

Ahern,P.R. [65]: Elementary methods in the theory of primes, Trans. Amer. Math. Soc., **118**, 1965, 221–242.

Albert,A.A. [30a]: The integers of normal quartic fields, Ann. of Math., (2) **31**, 1930, 481–418.

Albert,A.A. [30b]: A determination of the integers of all cubic fields, Ann. of Math., (2) **31**, 1930, 550–566.

Albert,A.A. [37]: Normalized integral bases of algebraic number fields, I, Ann. of Math., (2) **38**, 1937, 923–957.

Albert,A.A. [40]: On p-adic fields and rational division algebras, Ann. of Math., (2) **41**, 1940, 674–693.

Albis-Gonzalez,V.S. [73]: A remark on primitive roots and ramification, Rev. Colomb. Math., **7**, 1933, 93–98.

Albu,T. [79]: On a paper of Uchida concerning finite simple extensions of Dedekind domains, Osaka Math. J., **16**, 1979, 65–69.

Albu,T.,Nicolae,F. [95]: Heckesche Systeme von idealen Zahlen und Knesersche Körpererweiterungen, Acta Arith., **73**, 1995, 43–50.

Allen,S.,Pleasants,P.A.B. [80]: The number of different lengths of irreducible factorization of a natural number in an algebraic number field, Acta Arith., **36**, 1980, 59–86.

Amano,K. [77]: On the Galois cohomology groups of algebraic tori and Hasse's norm theorem, Bull. Fac. Gen. Ed. Gifu Univ., **13**, 1977, 185–190.

Amano,K. [79]: On the Hasse norm principle for a separable extension, Bull. Fac. Gen. Ed. Gifu Univ., **15**, 1979, 10–13.

Amano,S. [71]: Eisenstein equations of degree p in a $\mathfrak{p}$-adic fields, J. Fac. Sci. Univ. Tokyo, **18**, 1971, 1–21.

Amara,H. [81]: Groupes de classes et unité fondamentale des extensions quadratiques relatives à un corps quadratique imaginaire principal, Pacific J. Math., **96**, 1981, 1–12.

Amara,M. [79]: Sur le produit des conjugués, exterieurs au disque unité, de certains nombres algébriques, Acta Arith., **34**, 1979, 307–314.

Amberg,E.J. [97]: *Über die Körper, dessen Zahlen sich aus zwei Quadratwurzeln zusammensetzen*, Dissertation, Zürich 1897.

Amice,Y.,Fresnel,J. [72]: Fonctions zêta p-adiques des corps de nombres abéliens réels, Acta Arith., **20**, 1972, 353–384.

Amoroso,F. [95]: Sur des polynômes de petites mesures de Mahler, C.R. Acad. Sci. Paris, **321**, 1995, 11–14.

Amoroso,F. [96]: Algebraic numbers close to 1 and variants of Mahler's measure, J. Number Theory, **60**, 1996, 80–96.

Amoroso,F. [98]: Upper bound for the resultant and Diophantine applications, in: *Number Theory (Eger 1996)*, 23–36, de Gruyter 1998.

Amoroso,F.,David,S. [99]: Le problème de Lehmer en dimension supérieure, J. Reine Angew. Math., **513**, 1999, 145–179.

Amoroso,F.,Dvornicich,R. [00]: A lower bound for the height in abelian extensions, J. Number Theory, **80**, 2000, 260–272.

Amoroso,F.,Zannier,U. [00]: A relative Dobrowolski lower bound over abelian extensions, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., (4) **29**, 2000, 711–727.

Anderson,D.D., Anderson, D.F. [92]: Elasticity of factorizations in integral domains, J.Pure Appl. Algebra, **80**, 1992, 217–235; II, Houston J. Math., **20**, 1994, 1–15.

Anderson,D.D., Anderson, D.F., Chapman,S., Smith,W. [95]: Rational elasticity of factorizations in Krull domains, Proc. Amer. Math. Soc., **117**, 1993, 37–43.

Anderson,D.F.,Chapman,S.T. [00]: On the elasticities of Krull domains with finite cyclic divisor class group, Comm. Algebra, **28**, 2000, 2543–2553,

Anderson, D.F., Chapman,S.T., Smith,W.W. [94]: Overrings of half-factorial domains, Canad. Math. Bull., **37**, 1994, 437–442.

Anderson,D.F.,Pruis,P. [91]: Length functions on integral domains, Proc. Amer. Math. Soc., **113**, 1991, 933–937.

Anderson,G.W. [86]: Cyclotomy and an extension of the Taniyama group, Compositio Math., **57**, 1986, 153–217.

Anfert'eva,E.A.,Chudakov,N.G. [64]: On the minimas of the norm-function in imaginary quadratic fields, Dokl. Akad. Nauk SSSR, **159**, 1964, 1207–1209. (Russian)

Anfert'eva,E.A.,Chudakov,N.G. [70]: Effective estimates from below of the norms of ideals of an imaginary quadratic field, Mat. Sb., **82**, 1970, 55–66. (Russian)

Angell,L.O. [76]: A table of totally real cubic fields, Math. Comp., **30**, 1976, 184–187.

Ankeny,N.C. [51]: An improvement of an inequality of Minkowski, Proc. Nat. Acad. Sci. U.S.A., **37**, 1951, 711–716.

Ankeny,N.C. [52a]: A generalization of a theorem of Suetuna on Dirichlet series, Proc. Japan Acad. Sci., **28**, 1952, 289–295.

Ankeny,N.C. [52b]: Representation of primes by quadratic forms, Amer. J. Math., **74**, 1952, 913–919.

Ankeny,N.C.,Artin,E.,Chowla,S. [52]: The class number of real quadratic fields, Ann. of Math., (2) **78**, 1956, 51–61.

Ankeny,N.C.,Brauer,R.,Chowla,S. [52]: A note on the class numbers of algebraic number fields, Amer. J. Math., **78**, 1956, 51–61.

Ankeny,N.C.,Chowla,S. [49]: The class number of the cyclotomic field, Proc. Nat. Acad. Sci. U.S.A., **35**, 1949, 529–532.

Ankeny,N.C.,Chowla,S. [51]: The class number of the cyclotomic field, Canad. J. Math., **3**, 1951, 486–491.

Ankeny,N.C.,Chowla,S. [55]: On the divisibility of the class number of quadratic fields, Pacific J. Math., **5**, 1955, 321–324.

Ankeny,N.C.,Chowla,S. [62]: A further note on the class number of real quadratic fields, Acta Arith., **7**, 1962, 271–272.

Ankeny,N.C.,Chowla,S.,Hasse,H. [65]: On the class number of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., **217**, 1965, 217–220.

Ankeny,N.C.,Rogers,C.A. [51]: A conjecture of Chowla, Ann. of Math., (2) **53**, 1951, 541–555; (2) **58**, 1953, p.591.

Antoniadis,J.A. [83]: Über die Kennzeichnung zweiklassiger imaginär-quadratischer Zahlkörper durch Lösungen diophantischer Gleichungen, J. Reine Angew. Math., **339**, 1983, 27–81.

Aoki,N. [96]: Abelian fields generated by a Jacobi sum, Comment. Math. Univ. St. Paul, **45**, 1996, 1–21.

Appelgate,H.,Onishi,H. [82]: Periodic expansions of modules and its relation to units, J. Number Theory, **15**, 1982, 283–294.

Arai,M. [81]: On Voronoj's theory of cubic fields,I, Proc. Japan Acad. Sci., **57**, 1981, 226–229; II, 281–283.

Aramata,H. [31]: Über die Teilbarkeit der Zetafunktionen gewisser algebraischer Zahlkörper, Proc. Imp. Acad. Tokyo, **7**, 1931, 334–336.

Aramata,H. [33]: Über die Teilbarkeit der Dedekindschen Zetafunktionen, Proc. Imp. Acad. Tokyo, **9**, 1933, 31–34.

Aramata,H. [39]: Über die Eindeutigkeit der Artinschen L-Funktionen, Proc. Imp. Acad. Tokyo, **15**, 1939, 124–126.

Archinard,G. [74]: Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogène, Enseign. Math., (2) **20**, 1974, 179–203.

Archinard,G. [84]: Submodules of a torsion-free and finitely generated module over a Dedekind ring, Colloq. Math., **48**, 1984, 193–204.

Armitage,J.V. [67]: On a theorem of Hecke in number fields and function fields, Invent. math., **2**, 1967, 238–246.

Armitage,J.V. [72]: Zeta functions with a zero at $s = 1/2$, Invent. math., **15**, 1972, 199–205.

Armitage,J.V.,Fröhlich,A. [67]: Classnumbers and unit signatures, Mathematika, **14**, 1967, 94–98.

Arnaudon,M. [76]: Étude des normes dans les extensions galoisiennes de corps de nombres, C.R. Acad. Sci. Paris, **283**, 1976, 269–272.

Arndt,F. [58a]: Über die Anzahl der Genera der quadratischen Formen, J. Reine Angew. Math., **56**, 1858, 72–78.

Arndt,F. [58b]: Einfacher Beweis der Irreduzibilität einer Gleichung in der Kreisteilung, J. Reine Angew. Math., **56**, 1858, 178–181.

Arno,S. [92]: The imaginary quadratic fields of class number 4, Acta Arith., **60**, 1992, 321–334.

Arno,S.,Robinson,M.L.,Wheeler,F.S. [98]: Imaginary quadratic fields with small odd class number, Acta Arith., **83**, 1998, 295–330.

Arpaia,P.J. [68]: A note on quadratic Euclidean domains, Amer. Math. Monthly, **75**, 1968, 864–865.

Artin,E. [23]: Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann., **89**, 1923, 147–156.

Artin,E. [24]: Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg, **3**, 1924, 89–108.

Artin,E. [30a]: Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Abh. Math. Sem. Univ. Hamburg, **7**, 1930, 46–51.

Artin,E. [30b]: Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren, Abh. Math. Sem. Univ. Hamburg, **8**, 1930, 292–306.

Artin,E. [31]: Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, J. Reine Angew. Math., **164**, 1931, 1–11.

Artin,E. [32a]: Über Einheiten relativgaloischer Zahlkörper, J. Reine Angew. Math., **167**, 1932, 153–156.

Artin,E. [32b]: Über die Bewertungen algebraischer Körper, J. Reine Angew. Math., **167**, 157–159.

Artin,E. [50a]: Questions de base minimale dans la théorie des nombres algébriques, in: *Algébre et Théorie des Nombres*, Colloques du CNRS, **24**, 1950, 19–20.

Artin,E. [50b]: Remarques concernant la théorie de Galois, in: *Algébre et Théorie des Nombres*, Colloques du CNRS, **24**, 1950, 161–162.

Artin,E. [56]: Representatives of the connected component of the idèle class group, in: *Proceedings of the International Symposium on Algebraic Number Theory (Tokyo 1956)*, 51–54, Tokyo 1956.

Artin,E. [59]: *Theory of Algebraic Numbers*, Göttingen 1959.

Artin,E. [67]: *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, 1967.

Artin,E.,Tate,J. [68]: *Class Field Theory*, Benjamin 1968; 2nd ed. Addison–Wesley 1990.

Artin,E.,Whaples,G. [45]: Axiomatic characterization of fields by the product formula for valuations, Bull. Amer. Math. Soc., **51**, 1945, 469–492.

Artin,E.,Whaples,G. [46]: A note on axiomatic characterization of fields, Bull. Amer. Math. Soc., **52**, 1946, 245–247.

Arutyunyan,L.Z. [77]: Generators of the group of principal units of a cyclic p-extension of a regular local field, Zap. Nauchn. Sem. LOMI, **71**, 1977, 16–23. (Russian)

Arwin,A. [29]: On cubic fields, Ann. of Math., (2) **30**, 1929, 1–11.

Asano,K. [50]: Über Moduln und Elementarteilertheorie im Körper, in dem Arithmetik definiert ist, Japan J. Math., bf20, 1950, 55–71.

Avanesov,É.T. [79]: On the fundamental units of algebraic fields of degree n, Acta Arith., **35**, 1979, 175–185. (Russian)

Avanesov,É.T.,Billevich,K.K. [81]: Fundamental units of cubic fields of positive discriminants, Mat. Zametki, **29**, 1981, 801–812, 995. (Russian)

Ax,J. [62]: The intersection of norm groups, Trans. Amer. Math. Soc., **105**, 1962, 462–474.

Ax,J. [65]: On the units of an algebraic number field, Illinois J. Math., **9**, 1965, 584–589.

Ayoub,C.W. [69]: On finite primary rings and their groups of units, Compositio Math., **21**, 1969, 247–252.

Ayoub,R.G. [55]: On Selberg's lemma for algebraic number fields, Canad. J. Math., **7**, 1955, 138–143.

Ayoub,R.G. [58]: A mean value theorem for quadratic fields, Pacific J. Math., **8**, 1958, 23–27.

Ayoub,R.G. [67]: A note on the class number of imaginary quadratic fields, Math. Comp., **21**, 1967, 442–445.

Ayoub,R.G. [68]: On the coefficients of the zeta-function of an imaginary quadratic field, Acta Arith., **13**, 1968, 375–381.

Ayoub,R.G.,Chowla,S. [81]: On Euler's polynomial, J. Number Theory, **13**, 1981, 443–445.

Azizi,A. [97]: Sur la capitulation des 2-classes d'idéaux de $Q(\sqrt{d}, i)$, C.R. Acad. Sci. Paris, **325**, 127–130.

Azizi,A. [00]: Sur la capitulation de 2-classes d'idéaux de $k = Q(\sqrt{2pq}, i)$ où $p \equiv -q \equiv 1 \pmod 4$, Acta Arith., **94**, 2000, 383–399.

Azizi,A.,Mouhib,A. [01]: Sur le rang du 2-groupe de classes de $Q(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou un premier $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc., **353**, 2001, 2741–2752.

Azizi,A.,Mouhib,A. [03]: Capitulation des 2-classes d'idéaux de $Q(\sqrt{2}, \sqrt{d})$ oú d est un entier naturel sans facteurs carrés, Acta Arith., **109**, 2003, 27–63.

Azuhata,T. [84]: On the fundamental units and the class numbers of real quadratic fields, Nagoya Math. J., **95**, 1984, 125–135.

Azuhata,T.,Ichimura,H. [84]: On the divisibility problem of the class numbers of algebraic number fields, J. Fac. Sci. Univ. Tokyo, **30**, 1984, 579–585.

Baayen,P.C. [69]: $(C_2 \oplus C_2 \oplus C_2 \oplus C_{2n})!$ is true for odd n, Math. Centrum, Amsterdam, ZW 1969-006.

Baayen,P.C.,Emde Boas,P.van,Kruyswijk,D. [69]: A combinatorial problem on finite Abelian groups, III, Math. Centrum, Amsterdam, ZW 1969-008.

Babaev,G. [71]: An arithmetic proof of the infinity of prime ideals of degree ≥ 2, DAN Tadzhik. SSR, **14**, 1971, no.9, 3–6. (Russian)

Babaitsev,V.A. [80]: On the boundedness of Iwasawa's μ-invariant, Izv. Akad. Nauk SSSR, Ser. Mat., **44**, 1980, 3–23. (Russian)

Babaitsev,V.A. [81]: On the linear character of the behaviour of the Iwasawa μ invariant, Izv. Akad. Nauk SSSR, Ser. Mat., **45**, 1981, 691–703. (Russian)

Bachman,G. [66]: The decomposition of a rational prime in cyclotomic fields, Amer. Math. Monthly, **73**, 1966, 494–497.

Bachmann,P. [64]: *De unitatum complexarum theoria*, Berlin 1864, 23 pp.

Bae,S.H. [92]: Values of L-functions at $s = 0$, Archiv Math., **58**, 1992, 551–560.

Baily,A.M. [80]: On the density of discriminants of quartic fields, J. Reine Angew. Math., **315**, 1980, 190–210.

Baily,A.M. [81]: On octic fields of exponent 2, J. Reine Angew. Math., **328**, 1981, 33–38.

Baker,A. [66]: Linear forms in the logarithms of algebraic numbers, Mathematika, **13**, 1966, 204–216.

Baker,A. [69]: A remark on the class number of quadratic fields, Bull. London Math. Soc., **1**, 1969, 98–102.

Baker,A. [71a]: On the class-number of imaginary quadratic fields, Bull. Amer. Math. Soc., **77**, 1971, 678–684.

Baker,A. [71b]: Imaginary quadratic fields with class number 2, Ann. of Math., (2) **94**, 1971, 139–152.

Baker,A.,Schinzel,A. [71]: On the least integers represented by the genera of binary quadratic forms, Acta Arith., **18**, 1971, 137–144.

Baker,A.,Stark,H.M. [71]: On a fundamental inequality in number theory, Ann. of Math., (2) **94**, 1971, 190–199.

Baker,A.,Wüstholz,G. [93]: Logarithmic forms and group varieties, J. Reine Angew. Math., **442**, 1993, 19–62.

Balakrishnan,U. [86]: Extreme values of the Dedekind zeta function, Acta Arith., **46**, 1988, 199–210.

Baldisseri,N. [75]: Sulla lunghezza dell'algoritmo euclideo nei campi quadratici euclidici complessi, Boll. Un. Mat. Ital., (5), **12**, 1975, 333–347.

Ballieu,R. [54]: Factorisation des polynomes cyclotomiques modulo un nombre premier, Ann. Soc. Sci. Bruxelles, Sér.I, **68**, 1954, 140–144.

Barban,M.B. [62]: The "large sieve" of Ju.V.Linnik and limit theorem for the class-number of an imaginary quadratic field, Izv. Akad. Nauk SSSR, Ser. Mat., **26**, 1962, 563–580. (Russian)

Barban,M.B. [67]: On the density hypothesis of E.Bombieri, Dokl. Akad. Nauk SSSR, **172**, 1967, 999–1000. (Russian)

Barban,M.B.,Gordover,G. [66]: On the moments of the class-numbers of purely radical quadratic forms of negative determinant, Dokl. Akad. Nauk SSSR, **167**, 1966, 267–269. (Russian)

Barban,M.B.,Levin,B.V. [68]: Multiplicative functions on "shifted" prime numbers, Dokl. Akad. Nauk SSSR, **181**, 1968, 778–780. (Russian)

Barkan,P. [75]: Sur des sommes de caractéres liées aux nombre de classes des corps abéliens imaginaires, C.R. Acad. Sci. Paris, **281**, 1975, A887–890.

Barkan,P. [90]: Démonstration d'une conjecture de K.Yamamoto sur les sommes de Gauss biquadratiques, C.R. Acad. Sci. Paris, **310**, 1990, 69–72.

Barner,K. [67]: Zur Reziprozität quadratischer Charaktersummen in algebraischen Zahlkörpern, Monatsh. Math., **71**, 1967, 369–384.

Barner,K. [68]: Über die quaternäre Einheitsform in total reellen quadratischen Zahlkörpern, Monatsh. Math., **71**, 1967, 369–384.

Barner,K. [69]: Über die Werte der Ringklassen-L-Funktionen reell-quadratischer Zahlkörper an natürlichen Argumentstellen, J. Number Theory, **1**, 1969, 28–64.

Barner,K. [81]: On A.Weil's explicit formulas, J. Reine Angew. Math., **323**, 1981, 139–152.

Barrucand,P. [71]: Quelques propriétés des coefficients de séries L associés aux corps cubiques, C.R. Acad. Sci. Paris, **273**, 1971, 960–963.

Barrucand,P.,Cohn,H. [69]: Note on primes of type $x^2 + 32y^2$, class number and residuacity, J. Reine Angew. Math., **238**, 1969, 67–70.

Barrucand,P.,Cohn,H. [70]: A rational genus, class number divisibility and unit theorem for pure cubic fields, J. Number Theory, **2**, 1970, 7–21.

Barrucand,P.,Cohn,H. [73]: On some class-fields related to primes of type x^2+32y^2, J. Reine Angew. Math., **263/263**, 1973, 400–414.

Barrucand,P.,Laubie,F. [82]: Ramification modérée dans les corps de nombres de degré premier, Sém. Théor. Nombres Bordeaux, 1981/82, exp.13.

Barrucand,P.,Louboutin,S. [93]: Majoration et minoration du nombre de classes d'idéaux des corps réels purs de degré premier, Bull. London Math. Soc., **25**, 1993, 533–540.

Barrucand,P.,Loxton,J.,Williams,H.C. [87]: Some explicit upper bounds on the class numbers and regulator of a cubic field with negative discriminant, Pacific J. Math., **128**, 1987, 209–222.

Barsky,D. [77]: Fonctions zeta p-adiques d'une classe de rayon de corps totalement réels, Gr. Etud. Anal. Ultrametr., **5**, 1977/78, exp.23, 1–16.

Barsky,D. [83]: Sur la norme de certaines séries d"Iwasawa (une démonstration analytique p-adique du théorème de Ferrero-Washington), Study group on ultrametric analysis, **10**, 1982/83, no.1, exp.13, 1–44.

Bartels,H.J. [80]: Über Normen algebraischer Zahlen, Math. Ann., **251**, 191–212.

Bartels,H.J. [81a]: Zur Arithmetik in Diedergruppenerweiterungen, Math. Ann., **256**, 1981, 465–473.

Bartels,H.J. [81b]: Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen, J. Algebra, **70**, 1981, 179–199.

Bartz,K. [78]: On a theorem of Sokolovskiĭ, Acta Arith., **34**, 1978, 113–126.

Bartz,K. [85]: Some remarks on zero-free regions for Hecke-Landau zeta-functions, Discuss. Math., **7**, 1985, 113–117.

Bartz,K. [88]: An effective order of Hecke-Landau zeta-functions near the line $\sigma = 1$, I, Acta Arith., **50**, 1988, 183–193; II, **52**, 1989, 163–170; corr. **58**, 1991, p.211.

Bartz,K.,Fryska,T. [89]: An effective estimate for the density of zeros of Hecke-Landau zeta-functions, Acta Arith., **52**, 1989, 339–352.

Bartz,K.,Staś,W. [86]: On the order of Hecke-Landau zeta-functions near the line $\sigma = 1/2$, Funct. Approx. Comment. Math., **15**, 1986, 131–137.

Bass,H. [62]: Torsion free and projective modules, Trans. Amer. Math. Soc., **102**, 1962, 319–327.
Bass,H. [66]: The Dirichlet unit theorem, induced characters and Whitehead groups of finite group, Topology, **4**, 1966, 391–410.
Bass,H. [68]: *Algebraic K-theory*, Benjamin, New York 1968.
Bass,H.,Milnor,J.,Serre,J.P. [67]: Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), Inst. Hautes Études Sci., Publ. Math., **33**, 1967, 59–137.
Bauer,H. [71]: Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math., **248**, 1971, 42–46.
Bauer,H. [72]: Die 2-Klassenzahl spezieller quadratischer Zahlkörper, J. Reine Angew. Math., **252**, 1972, 79–81.
Bauer,M. [16a]: Zur Theorie der algebraischen Zahlkörper, Math. Ann., **77**, 1916, 353–356.
Bauer,M. [16b]: Über zusammengesetzte Zahlkörper, Math. Ann., **77**, 1916, 357–361.
Bauer,M. [19a]: Bemerkungen über die Differente des algebraischen Zahlkörpers, Math. Ann., **79**, 1919, 321–322.
Bauer,M. [19b]: Zur Theorie der Fundamentalgleichung, J. Reine Angew. Math., **149**, 1919, 86–96.
Bauer,M. [20]: Bemerkungen über die Zusammensetzung der algebraischen Zahlkörper, J. Reine Angew. Math., **150**, 1920, 185–188.
Bauer,M. [21a]: Über relativ-Galoissche Zahlkörper, Math. Ann., **83**, 1921, 70–73.
Bauer,M. [21b]: Über die Differente eines algebraischen Zahlkörpers, Math. Ann., **83**, 1921, 74–76.
Bauer,M. [21c]: Beweis von einigen bekannten Sätzen über zusammengesetzte Körper ohne Anwendung der Idealtheorie, Jahresber. Deutsch. Math.-Verein., **30**, 1921, 186–188.
Bauer,M. [22]: Die Theorie der p-adischen bzw. $\mathfrak{p}$-adischen Zahlen und die gewöhnlichen algebraischen Zahlkörpern, Jahresber. Deutsch. Math.-Verein., **14**, 1922, 244–249; **20**, 1924, 94–97.
Bauer,M. [23]: Verschiedene Bemerkungen über die Differente und die Diskriminante eines algebraischen Zahlkörpers, Math. Z., **16**, 1923, 1–12.
Bauer,M. [24]: Über die Erweiterungen des Körpers der p-adischen Zahlen zu einem algebraisch abgeschlossenen Körper, Math. Z., **19**, 1924, 308–312.
Bauer,M. [36]: Bemerkungen zum Hensel-Oreschen Hauptsatze, Acta Sci. Math. (Szeged), **8**, 1936, 64–67.
Bauer,M. [37]: Bemerkungen über die Galoissche Gruppe einer Gleichung, Math. Ann., **114**, 1937, 352–354.
Bauer,M. [39]: Zur Theorie der Kreiskörper, Acta Sci. Math. (Szeged), **9**, 1939, 110–112.
Bauer,M. [40a]: Über zusammengesetzte relativ Galoissche Körper, Acta Sci. Math. (Szeged), **9**, 1940, 206–211.
Bauer,M. [40b]: Über die Zusammensetzung algebraischer Zahlkörper, Acta Sci. Math. (Szeged), **9**, 1940, 212–217.
Bauer,M.,Chebotarev,N.G. [28]: p-adischer Beweis des zweiten Hauptsatzes von Herrn Ore, Acta Sci. Math. (Szeged), **4**, 1928, 56–57.
Bayad,A.,Bley,W.,Cassou-Noguès,Ph. [96]: Sommes arithmétiques et éléments de Stickelberger, J. Algebra, **179**, 1996, 145–190.
Bayer,P.,Neukirch,J. [79]: On values of zeta functions and l-adic Euler characteristic, Invent. math., **50**, 1978/79, 35–64.

Bayer,P.,Rio,A. [99]: Dyadic exercises for octahedral extensions, J. Reine Angew. Math., **517**, 1999, 1–17.

Bazylewicz,A. [76]: On the product of the conjugates of an algebraic integer outside the unit circle of an algebraic integer, Acta Arith., **30**, 1976, 43–61.

Bazylewicz,A. [82]: Traces of monomials in algebraic numbers, Acta Arith., **41**, 1982, 101–116.

Beaumont,R.A.,Pierce,R.S. [61]: Subrings of algebraic number fields, Acta Sci. Math. (Szeged), **22**, 1961, 202–216.

Beeger,N.G.W.H. [19]: Über die Teilkörper des Kreiskörpers $K(\zeta_n)$, Proc. Akad. Wet. Amsterdam, **21**, 1919, 454–465, 758–773, 774–779.

Beeger,N.G.W.H. [20]: Bestimmung der Klassenzahl der Ideale aller Unterkörper des Kreiskörpers der ζ_m, wo m durch mehr als eine Primzahl teilbar ist. Proc. Akad. Wet. Amsterdam, **22**, 1920, 331–250, 395–414; corr., **23**, 1922, 1399–1401.

Behnke,H. [23]: Ueber analytische Funktionen und algebraische Zahlen, Abh. Math. Sem. Univ. Hamburg, **2**, 1923, 81–111.

Behrbohm,H.,Rédei,L. [36]: Der Euklidische Algorithmus in quadratischen Körpern, J. Reine Angew. Math., **174**, 1936, 192–205.

Belabas,K. [97]: A fast algorithm to compute cubic fields, Math. Comp., **66**, 1997, 1213–1237.

Belabas,K. [99]: On the mean 3-rank of quadratic fields, Compositio Math.. **118**, 1999, 1–9.

Belabas,K.,Fouvry,E. [99]: Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, Duke Math. J., **98**, 1999, 217–268.

Belcher,P. [74]: Integers expressible as sums of distinct units, Bull. London Math. Soc., **6**, 1974, 66–68.

Belcher,P. [75]: A test for integers being sums of distinct units applied to cubic fields, J. London Math. Soc., **12**, 1975/76, 141–148.

Benjamin,E. [93]: Remarks concerning the 2-Hilbert class field of imaginary quadratic number fields, Bull. Austral. Math. Soc., **48**, 1993, 379–383.

Benjamin,E. [99]: On the second Hilbert 2-class field of real quadratic number fields with 2-class group isomorphic to $(2, 2^n)$, $n \geq 2$, Rocky Mountain J. Math., **29**, 1999, 763–788.

Benjamin,E.,Lemmermeyer,F.,Snyder,C. [97]: Imaginary quadratic fields k with cyclic $Cl_2(k^1)$, J. Number Theory, **67**, 1997,229–245.

Benjamin,E.,Lemmermeyer,F.,Snyder,C. [98a]: Imaginary quadratic fields k with $Cl_2(k) \approx (2, 2^m)$ and rank $Cl_2(k^1) = 2$, Pacific J. Math., **198**, 2001, 15–31.

Benjamin,E.,Lemmermeyer,F.,Snyder,C. [98b]: Real quadratic fields with abelian 2-class field tower, J. Number Theory, **73**, 1998, 182–194.

Benjamin,E.,Sanborn,F.,Snyder,C. [94]: Capitulation in unramified quadratic extensions of real quadratic number fields, Glasgow Math. J., **36**, 1994, 385–392.

Benjamin,E.,Snyder,C. [95]: Real quadratic number fields with 2-class group of type $(2, 2)$, Math. Scand., **76**, 1995, 161–178.

Bennett,A.A. [23]: Some algebraic analogs in matric theory, Ann. of Math., (2) **23**, 1923, 91–96.

Benson,C.T.,Weber,B.T. [73]: Computing units in certain orders of algebraic integers, J. Number Theory, **5**, 1973, 99–107.

Bérczes,A. [00]: On the number of solutions of index form equations, Publ. Math. Debrecen, **56**, 2000, 251–262.

Berg,E. [35]: Über die Existenz eines Euklidischen Alorithmus in quadratischen Zahlkörpern, Fysiogr. Sällsk. Lund Förh., **5**, 1935, 1–6.

Bergé,A.M. [72]: Sur l'arithmétique d'une extension diédrale, Ann. Inst. Fourier, **22**, 1972, no.2, 31–59.

Bergé,A.M. [78]: Arithmétique d'une extension galoisienne à groupe des d'inertie cyclique, Ann. Inst. Fourier, **28**, 1978, no.4, 17–44.
Bergé,A.M. [81]: A propos du genre de l'anneau des entiers d'une extension, Publ. Math. Fac. Sci. Besançon, 1979/80 et 1980/81, 9 pp.
Bergé,A.-M.,Martinet,J. [89]: Notions relatives de régulateurs et de hauteurs, Acta Arith., **54**, 1989, 155–170.
Bergé,A.-M.,Martinet,J.,Olivier,M. [90]: The computation of sextic fields with a quadratic subfield, Math. Comp., **54**, 1990, 869–884.
Berger,R.I. [92]: Hasse's class number product formula for generalized Dirichlet fields and other types of number fields, Manuscripta Math., **76**, 1992, 397–406.
Berger,T.R.,Reiner,I. [75]: A proof of the normal basis theorem, Amer. Math. Monthly, **82**, 1975, 915–918.
Bergmann,G. [65]: Untersuchungen zue Einheitengruppe in den totalkomplexen Körpern sechsten Grades (über P) im Rahmen der "Theorie der Netze", Math. Z., **161**, 1965, 349–364.
Bergmann,H. [66a]: Über Eulers Beweis des grossen Fermatschen Satzes für den Exponenten 3, Math. Ann., **164**, 1966, 159–175.
Bergmann,H. [66b]: Zur numerischen Bestimmung einer Einheitenbasis, Math. Ann., **166**, 1966, 103–105.
Bergmann,H. [66c]: Beispiel numerischer Einheitenbestimmung, Math. Ann., **167**, 1966, 143–168.
Bergström,H. [37]: Über die Methode von Woronoj zur Berechnung einer Basis eines kubischen Zahlkörpers, Ark. Mat., **25B**, 1937, No.26, 1–8.
Bergström,H. [44]: Die Klassenzahlformel für reelle quadratische Zahlkörper mit zusammengesetzter Diskriminante als Produkt verallgemeinerter Gaussscher Summen, J. Reine Angew. Math., **186**, 1944/45, 91–115.
Berndt,B.C. [69]: A note on the number of integral ideals of bounded norm in a quadratic number field, Bull. Amer. Math. Soc., **75**, 1969, 1283–1285.
Berndt,B.C. [70]: On the zeros of a class of Dirichlet series, I, Illinois J. Math., **14**, 1970, 244–258; II, 678–691.
Berndt,B.C. [71a]: The number of zeros of the Dedekind zeta-function on the critical line, J. Number Theory, **3**, 1971, 1–6.
Berndt,B.C. [71b]: On the average order of a class of arithmetical functions, J. Number Theory, **3**, 1971, 184–203; II, 288–305.
Berndt,B.C. [73]: Character transformation formulae similar to those of Dedekind eta-function, Proc. Symposia Pure Math., **24**, 1973, 9–30.
Berndt,B.C. [75]: Identities involving the coefficients of a class of Dirichlet series, VII, Trans. Amer. Math. Soc., **201**, 1975, 247–261.
Berndt,B.C.,Evans,R.J. [77]: Dedekind sums and class numbers, Monatsh. Math., **84**, 1977, 265–273.
Berndt,B.C.,Evans,R.J. [81]: The determination of Gauss sums, Bull. Amer. Math. Soc., (N.S.) **5**, 1981, 107–129.
Berndt,B.C.,Evans,R.J.,Williams,K.S. [98]: *Gauss and Jacobi Sums*, J.Wiley 1998.
Bernstein,L. [71]: *The Jacobi-Perron Algorithm, its Theory and Applications*, Lecture Notes in Math., **207**, Springer 1971.
Bernstein,L. [75a]: Units and their norm equation in real algebraic number fields of any degree, Symposia Math., **15**, 1975, 307–340.
Bernstein,L. [75b]: Truncated units in infinitely many algebraic number fields of degree $n \geq 4$, Math. Ann., **213**, 1975, 275–279.
Bernstein,L. [77]: Gaining units from units, Canad. J. Math., **29**, 1977, 93–106.
Bernstein,L. [78a]: An algorithm for Halter-Koch units, Michigan J. Math., **25**, 1978, 371–377.
Bernstein,L. [78b]: Applications of units, J. Number Theory, **10**, 1978, 354–383.

Bernstein,L.,Hasse,H. [75]: Ein formales Verfahren zur Herstellung parameterabhängiger Scharen quadratischer Grundeinheiten, J. Reine Angew. Math., **276**, 1975, 206–212.

Bertin,M.-J. [91]: Une mesure de Mahler explicite, C.R. Acad. Sci. Paris, **333**, 2001, 1–3.

Bertin,M.J.,Decomps-Guilloux,A.,Grandet-Hugot,M.,Pathiaux-Delefosse,M., Schreiber,J.-P. [92]: *Pisot and Salem Numbers*, Birkhäuser 1992.

Bertin,M.-J.,Pathiaux-Delefosse,M. [89]: *Conjecture de Lehmer et petits nombres de Salem*, Kingston 1989.

Bertrandias,F. [65]: Ensembles remarquables d'adèles algébriques, Bull. Soc. Math. France, Mém. **4**, 1965.

Bertrandias,F. [78]: Entiers d'une p-extension cyclique d'un corps local, C.R. Acad. Sci. Paris. **286**, 1978, A1083–1086.

Bertrandias,F. [79]: Decomposition du Galois-module des entiers d'une extension cyclique de degré premier d'un corps des nombres ou d'un corps local, Ann. Inst. Fourier, **29**, 1979, no.1, 33–48.

Bertrandias,F.,Bertrandias,J.P.,Ferton,M.J. [72]: Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, C.R. Acad. Sci. Paris, **274**, 1972, A1330–1333.

Bertrandias,F.,Payan,J.J. [72]: Γ-extensions et invariants cyclotomiques, Ann. Sci. École Norm. Sup., (4) **5**, 1972, 517–543.

Berwick,W.E.H. [13]: The classification of ideal numbers that depend on a cubic irrationality, Proc. London Math. Soc., (2) **12**, 1913, 393–429.

Berwick,W.E.H. [24]: On cubic fields with a given discriminant, Proc. London Math. Soc., (2), **23**, 1924, 359–378.

Berwick,W.E.H. [27]: *Integral Bases*, Cambridge 1927. [Reprint: Stechert-Hafner 1964.]

Berwick,W.E.H. [32]: Algebraic number fields with two independent units, Proc. London Math. Soc., (2) **34**, 1932, 360–378.

Berwick,W.E.H. [34]: The classification of ideal numbers in a cubic field, Proc. London Math. Soc., (2) **38**, 1934, 217–242.

Besicovitch,A.S. [40]: On the linear independence of fractional powers of integers, J. London Math. Soc., **15**, 1940, 3–6.

Bessassi,S. [03]: Bounds for the degrees of CM-fields of class number one, Acta Arith., **106**, 2003, 213–245.

Beukers,F.,Schlickewei,H.P. [96]: The equation $x + y = 1$ in finitely generated groups, Acta Arith., **78**, 1996, 179–199.

Bhandari,S.K.,Nanda,V.C. [79]: Ideal matrices for relative extensions, Abh. Math. Sem. Univ. Hamburg, **49**, 1979, 3–17.

Bhaskaran,M. [71]: A new proof for the law of decomposition in a general cyclotomic field, Archiv Math., **22**, 1971, 62–64.

Bhaskaran,M. [74]: Some remarks on the decomposition of a rational prime in a Galois extension, Acta Arith., **26**, 1974, 101–104.

Bickmore,C.F. [93]: Tables connected with the Pellian equation, British Association Report, **53**, 1893, 73–120.

Bilhan,M. [81]: Théorème de Bauer dans les corps globaux, Bull. Sci. Math., (2) **105**, 1981, 299–303.

Billevich,K.K. [56]: On units of algebraic fields of degree 3 and 4, Mat. Sb., **40**, 1956, 123–136; corr.: **48**, 1959, p.256. (Russian)

Birch,B.J. [69]: Weber's class invariants, Mathematika, **16**, 1969, 283–294.

Birch,B.J.,Merriman,J.R. [72]: Finiteness theorems for binary forms with given discriminant, Proc. London Math. Soc., (3) **24**, 1972, 385–394.

Birch,B.J.,Swinnerton-Dyer,H.P.F. [75]: The Hasse problem for rational surfaces, J. Reine Angew. Math., **274/275**, 1975, 164–174.

Bird,R.F.,Parry,C.J. [76]: Integral bases for bicyclic biquadratic fields over quadratic subfields, Pacific J. Math., **66**, 1976, 29–36.

Biró,A. [03a]: Yokoi's conjecture, Acta Arith., **106**, 2003, 85–104.

Biró,A. [03b]: Chowla's conjecture, Acta Arith., **107**, 2003, 179–194.

Bitimbaev,T.S. [68]: Korkin's sum and its connection with the class-number of imaginary quadratic fields, Izv. Akad. Nauk Kazakh. SSR, 1968, no.1, 1–6. (Russian)

Blanksby,P.E. [69]: A note on algebraic integers, J. Number Theory, **1**, 1969, 155–160.

Blanksby,P.E. [70]: A metric inequality associated with valuated fields, Acta Arith., **17**, 1970, 217–225.

Blanksby,P.,Lloyd-Smith,C.W.,McAuley,M.J. [89]: On diameters of algebraic integers, Acta Arith., **52**, 1989, 1–9.

Blanksby,P.,Loxton,J. [78]: A note on the characterization of CM-fields, J. Austral. Math. Soc., **26**, 1978, 26–30.

Blanksby,P.E.,Montgomery,H.L. [71]: Algebraic integers near the unit circle, Acta Arith., **18**, 1971, 355–369.

Blasius,D. [86]: On the critical values of Hecke L-series, Ann. of Math., (2) **124**, 1986, 23–63.

Bley,W. [95]: A Leopoldt-type result for rings of integers of cyclotomic extensions, Canad. Math. Bull., **38**, 1995, 141–148.

Bloom,J.R. [79]: On the invariants of some Z_l-extensions, J. Number Theory, **11**, 1979, 239–256.

Bloom,J.R.,Gerth,F.III [81]: The Iwasawa invariant μ in the composite of two Z_l-extensions, J. Number Theory, **13**, 1981, 262–267.

Bölling,R. [79]: Bemerkungen über Klassenzahlen und Summen von Jacobi-Symbolen, Math. Nachr., **90**, 1979, 159–172.

Bombieri,E.,Mueller,J.,Poe,M. [97]: The unit equation and the cluster principle, Acta Arith., **79**, 1997, 361–369.

Bond,R.J. [81]: Some results on the capitulation problem, J. Number Theory, **13**, 1981, 246–254.

Borel,A. [77]: Cohomologie de SL_n et valeurs de fonctions zeta aux points entiers, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., (4) **4**, 1977, 613–636.

Borel,A.,Chowla,S.,Herz,C.S.,Iwasawa,K.,Serre,J.P. [66]: *Seminar on Complex Multiplication*, Lecture Notes in Math., **21**, Springer 1966.

Borevich,Z.I. [57]: On the proof of the principal ideal theorem, Vestnik LGU, **12**, 1957, no.13, 5–8. (Russian)

Borevich,Z.I. [64]: Multiplicative group of a regular local field with a cyclic operator group, Izv. Akad. Nauk SSSR, Ser. Mat., **28**, 1964, 707–712. (Russian)

Borevich,Z.I. [65a]: On the multiplicative group of cyclic p-extensions of a local field, Trudy Mat. Inst. Steklov., **80**, 1965, 16–29; II, Vestnik LGU, **20**, 1965, no.13, 5–12. (Russian)

Borevich,Z.I. [65b]: On the group of principal units of a normal p-extension of a regular local field, Trudy Mat. Inst. Steklov., **80**, 1965, 30–44. (Russian)

Borevich,Z.I. [67]: On groups of principal units of p-extensions of a local field, Dokl. Akad. Nauk SSSR, **173**, 1967, 253–255. (Russian)

Borevich,Z.I.,Gerlovin,É.I. [76]: Structure of the group of principal units of a cyclic p-extension of a local field, Zap. Nauchn. Sem. LOMI, **57**, 1976, 51–63. (Russian)

Borevich,Z.I.,Shafarevich,I.R. [64]: *Number Theory*, Moskva 1964 (Russian); 2nd ed. Moskva 1985, 3rd ed. Moskva 1985. [English translation: Academic Press 1966; French translation: Gauthier–Villars 1967, reprint 1993; German translation: Birkhäuser 1966.]

Borevich,Z.I.,Skopin,A.I. [65]: Extensions of a local field with a normal basis for the principal units, Trudy Mat. Inst. Steklov., **80**, 1965, 45–50. (Russian)

Borevich,Z.I.,Vostokov,S.V. [73]: The ring of integral elements of an extension of prime degree of a local field as a Galois module, Zap. Nauchn. Sem. LOMI, **31**, 1973, 24–37. (Russian)

Bosma,W.,de Smit,B. [01]: Class number relations from a computational point of view, J. Symbolic Comp., **31**, 2001, 97–112.

Bourbaki,N. [61/65]: *Algèbre commutative*, (fasc. 27,28, 30 and 31 of *Éléments de mathématique*), Hermann, Paris 1961–1965.

Boutteaux,G.,Louboutin,S. [02a]: The class number one problem for some non-normal sextic CM-fields, in: *Analytic Number Theory, Beijing-Kyoto 1999*, 27–37. Kluwer 2002.

Boutteaux,G.,Louboutin,S. [02b]: The class number one problem for the non-normal sextic CM-fields, Acta Math. Inf. Univ. Ostrava, **10**, 2002, 3–23.

Bouvier,L. [71]: Sur le 2-groupe des classes au sens restreint de certaines extensions biquadratiques de Q, C.R. Acad. Sci. Paris, **272**, 1971, A193–196.

Bouvier,L.,Payan,J.J. [75]: Modules sur certains anneaux de Dedekind, J. Reine Angew. Math., **274/275**, 1975, 278–286.

Bouvier,L.,Payan,J.J. [79]: Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p,p), Ann. Inst. Fourier, **29**, 1979, no.1, 171–187.

Boyd,D.W. [77]: Pisot sequences which satisfy no linear recurrence, Acta Arith., **32**, 1977, 89–98.

Boyd,D.W. [80]: Reciprocal polynomials having small Mahler measure, Math. Comp., **35**, 1980, 1361–1377; II, **53**, 1989, 355–357.

Boyd,D.W. [81a]: Speculations concerning the range of Mahler's measure, Canad. Math. Bull., **24**, 1981, 453–469.

Boyd,D.W. [81b]: Kronecker's theorem and Lehmer's problem for polynomials in several variables, J. Number Theory, **13**, 1981, 116–120.

Boyd,D.W. [85]: The maximal modulus of an algebraic integer, Math. Comp., **45**, 1985, 243–249.

Boyd,D.W. [86a]: Perron units which are not Mahler measures, Ergodic Theory, Dynam. Systems, **6**, 1986, 485–488.

Boyd,D.W. [86b]: Inverse problems for Mahler's measure, In: *Diophantine Analysis, (Kensington 1985)*, 147–158, London Math. Soc. Lecture Note Ser., **109**, Cambridge, 1986.

Boyd,D.W. [98a]: Mahler's measure and special values of L-functions, Experiment Math., **7**, 1998, 37–82.

Boyd,D.W. [98b]: Uniform approximation to Mahler's measure in several variables, Canad. Math. Bull., **41**, 1998, 125–128.

Boyd,D.W. [99]: Mahler's measure and special values of L-functions — some conjectures, in: *Number Theory in Progress*, **I**, 27–34, de Gruyter 1999.

Boyd,D.W. [02]: Mahler's measure and invariants of hyperbolic manifolds, in: *Number Theory for the Millenium*, **I**, 127–143, Peters 2002.

Boyd,D.W.,Kisilevsky,H. [72]: On the exponent of the ideal class groups of complex quadratic fields, Proc. Amer. Math. Soc., **31**, 1972, 433–436.

Boyd,D.W.,Villegas,F.R. [02]: Mahler's measure and the dilogarithm,I, Canad. J. Math., **54**, 2002, 468–492.

Brandal,W. [79]: *Commutative Rings whose Finitely Generated Modules Decompose*, Lecture Notes in Math., **723**, Springer 1979.

Brandis,A. [65]: Über die multiplikative Struktur von Körpererweiterungen, Math. Z., **87**, 1965, 71–73.

Brattström,G. [82]: Jacobi-sum Hecke characters of a totally real abelian field, Sém. Théor. Nombres Bordeaux, 1981/82, exp.22.

Brattström,G.,Lichtenbaum,S. [84]: Jacobi-sum Hecke characters of imaginary quadratic fields, Compositio Math., **53**, 1984, 277–302.
Brauer,R. [47a]: On the zeta-functions of algebraic number fields, Amer. J. Math., **69**, 1947, 243–250; II, **72**, 1950, 739–746.
Brauer,R. [47b]: On Artin's L-series with general group characters, Ann. of Math., (2) **48**, 1947, 502–514.
Brauer,R. [51]: Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, Math. Nachr., **4**, 1950/51, 158–174.
Brauer,R. [73]: A note on zeta-functions of algebraic number fields, Acta Arith., **24**, 1973, 325–327.
Bredikhin,B.M. [58]: Free semigroups of numbers with power densities, Mat. Sb., **46**, 1958, 143–158. (Russian)
Bremner,A. [78]: Some cubic surfaces with no rational points, Math. Proc. Cambridge Philos. Soc., **84**, 1978, 219–223.
Bremner,A. [88]: On power bases in cyclotomic fields, J. Number Theory, **28**, 1988, 288–298.
Brentjes,A.J. [81]: A two-dimensional continued fraction algorithm for best approximations with an application in cubic number fields, J. Reine Angew. Math., **326**, 1981, 18–44.
Breusch,R. [51]: On the distribution of the roots of a polynomial with integral coefficients, Proc. Amer. Math. Soc., **3**, 1951, 939–941.
Brill,A. [77]: Ueber die Discriminante, Math. Ann., **12**, 1877, 87–89.
Brink,J.R.,Gold,R. [87]: Class field tower of imaginary quadratic fields, Manuscripta Math., **57**, 1987, 425–450.
Brinkhuis,J. [81a]: *Embedding problems and Galois modules*, Ph.D. thesis, Leiden 1981.
Brinkhuis,J. [81b]: Symmetries d'un module Galoisien, Sém. Théor. Nombres Bordeaux, 1981/82, exp.44.
Brinkhuis,J. [83]: Normal integral bases and embedding problems, Math. Ann., **264**, 1983, 537–543.
Brinkhuis,J. [84]: Galois modules and embedding problems, J. Reine Angew. Math., **346**, 1984, 141–165.
Brinkhuis,J. [87]: Normal integral bases and complex conjugation, J. Reine Angew. Math., **375/376**, 1987, 157–166.
Brinkhuis,J. [95]: Normal integral bases and the Spiegelungssatz of Scholz, Acta Arith., **69**, 1995, 1–9.
Browkin,J. [63]: On the generalized class field tower, Bull. Acad. Pol. Sci., sér. sci. math. astr. phys., **11**, 1963, 143–145.
Brown,E. [72]: The class number of $Q(\sqrt{-p})$ for $p \equiv 1 \pmod 8$, a prime, Proc. Amer. Math. Soc., **31**, 1972, 381–383.
Brown,E. [73]: The power of 2 dividing the class-number of a binary quadratic discriminant, J. Number Theory, **5**, 1973, 413–419.
Brown,E. [74a]: Class number of complex quadratic fields, J. Number Theory, **6**, 1974, 185–191.
Brown,E. [74b]: Class number of real quadratic fields, Trans. Amer. Math. Soc., **190**, 1974, 99–107.
Brown,E. [75]: Class numbers of quadratic fields, Symposia Math., **15**, 1975, 403–411.
Brown,E. [81]: The class-number of $Q(\sqrt{-pq})$, for $p \equiv -q \equiv 1 \pmod 4$ primes, Houston J. Math.. **7**, 1981, 497–505.
Brown,E. [83]: The class number and fundamental unit of $\mathbb{Q}(\sqrt{2p})$ for $p \equiv 1 \pmod 4$, J. Number Theory, **16**, 1983, 95–99.

Brown,E.,Parry,C.J. [73]: Class numbers of imaginary quadratic fields having exactly three discriminantial divisors, J. Reine Angew. Math., **260**, 1973, 31–34.
Brown,E.,Parry,C.J. [74]: The imaginary bicyclic biquadratic fields with class numbers 1, J. Reine Angew. Math., **266**, 1974, 118–120.
Brown,K.S. [74]: Euler characteristic of discrete groups and G-spaces, Invent. math., **27**, 1974, 229–264.
Brown,M.L. [87]: Relative heights and a density version of a theorem of Samuel, Quart. J. Math., Oxford ser., (2) **38**, 1987, 1–11.
Bruckner,G. [66]: Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind, Math. Nachr., **32**, 1966, 317–326.
Bruckner,G. [68]: Charakterisierung der in algebraischen Zahlkörpern voll zerlegten Primzahlen, Math. Nachr., **36**, 1968, 153–159.
Bruegeman,S. [01]: Septic number fields which are ramified only at one small prime, J. Symbolic Comp., **31**, 2001, 549–555.
Brumer,A. [65]: Ramification and class towers of number fields, Michigan J. Math., **12**, 1965, 129–131.
Brumer,A. [67]: On the units of algebraic number fields, Mathematika, **14**, 1967, 121–124.
Brumer,A. [69]: On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Japan, **21**, 1969, 357–358.
Brumer,A.,Rosen,M. [63]: Class number and ramification in number fields, Nagoya Math. J., **23**, 1963, 97–101.
Brunotte,H. [80]: Bemerkungen zu einer metrischen Invariante algebraischer Zahlkörper, Monatsh. Math., **90**, 1980, 171–184.
Brunotte,H. [83]: Zur Zerlegung totalpositiver Zahlen in Ordnungen totalreeller algebraischer Zahlkörper, Archiv Math., **41**, 1983, 502–503.
Brunotte,H.,Halter-Koch,F. [79]: Zur Einheitenberechnung in totalreellen kubischen Zahlkörpern nach Godwin, J. Number Theory, **11**, 1979, 552–559.
Brunotte,H.,Halter-Koch,F. [81a]: Metrische Kennzeichnung von Erzeugenden für Einheitengruppen vom Rang 1 oder 2 in algebraischen Zahlkörpern, J. Number Theory, **13**, 1981, 320–333.
Brunotte,H.,Halter-Koch,F. [81b]: Grundeinheitensysteme algebraischer Zahlkörper mit vorgegebener Verteilung der Konjugiertenbeträge, Archiv Math., **37**, 1981, 512–513.
Buchmann,J. [90]: A subexponential algorithm for the determination of class groups and regulators of algebraic number fields, Séminaire de Théorie des Nombres, Paris 1988/89, 27–41, Progress Math., **91**, Birkhäuser 1990.
Buchmann,J.,Ford,D. [89]: On the computation of totally real quartic fields of small discriminant, Math. Comp., **52**, 1989, 161–174.
Buchmann,J.,Ford,D.,Pohst,M. [93]: Enumeration of quartic fields of small discriminant, Math. Comp., **61**, 1993, 873–879.
Buell,D.A. [99]: The last exhaustive computation of class groups of complex quadratic number fields, in *Number Theory (Ottawa 1996)*, 35–53, Amer. Math. Soc. 1999.
Buell,D.A.,Williams,H.C.,Williams,K.S. [77]: On the imaginary bicyclic biquadratic fields with class-number 2, Math. Comp., **31**, 1977, 1034–1042.
Bugeaud,Y. [98]: Algebraic numbers close to 1 in non-Archimedean metrics, Ramanujan J., **2**, 1998, 449–457.
Bugeaud,Y.,Győry,K. [96a]: Bounds for the solutions of unit equations, Acta Arith., **74**, 1996, 67–80.
Bugeaud,Y.,Győry,K. [96b]: Bounds for the solutions of Thue-Mahler equations and norm-form equations, Acta Arith., **74**, 1996, 273–292.

Bugeaud,Y.,Mignotte,M.,Normandin,F. [95]: Nombres algébrique de petit mesure et formes linéaires en un logarithme, C.R. Acad. Sci. Paris. **321**, 1995, 517–522.
Buhler,J.P. [78]: *Icosahedral Galois Representations*, Lecture Notes in Math., **654**, Springer 1978.
Buhler.J.P.,Crandall,R.,Ernvall,R.,Metsänkylä,T., [93]: Irregular primes and cyclotomic invariants to four million, Math. Comp., **61**, 1993, 151–153.
Buhler,J.,Crandall,R.,Ernvall,R.,Metsänkylä,T., Shokrollah,M.A. [01]: Irregular primes and cyclotomic invariants to 12 million, J.Symbolic Computation, **31**, 2001, 89–96.
Buhler,J.P.,Crandall,R.,Sompolski,R.W. [92]: Irregular primes to one million, Math. Comp., **59**, 1992, 717–722.
Buhler,J.P.,Gross,B.H.,Zagier,D. [85]: On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3, Math. Comp., **44**, 1985, 473–485.
Bullig,G. [36]: Die Berechnung der Grundeinheit in den kubischen Körpern mit negativer Diskriminante, Math. Ann., **112**, 1936, 325–394.
Bullig,G. [38]: Ein periodisches Verfahren zur Berechnung eines Systems von Grundeinheiten in den total reellen kubischen Körpern, Abh. Math. Sem. Univ. Hamburg, **12**, 1938, 369–411.
Bulota,K. [63]: Some theorems on the density of Hecke's Z-functions, Lit. Mat. Sb., **3**, 1963, 29–50. (Russian)
Bulota,K. [64]: On Hecke's Z-functions and the distribution of primes in an imaginary quadratic field, Lit. Mat. Sb., **4**, 1964, 309–328.
Bumby,R.T. [67]: Irreducible integers in Galois extensions, Pacific J. Math., **22**, 1967, 221–229.
Bumby,R.T.,Dade,E.C. [67]: Remark on a problem of Niven and Zuckerman, Pacific J. Math., **22**, 1967, 15–18.
Bundschuh,P.,Hock,A. [69]: Bestimmung aller imaginär-quadratischen Zahlkörper der Klassenzahl Eins mit Hilfe eines Satzes von Baker, Math. Z., **111**, 1969, 191–204.
Burns,D.J. [91]: Factorisability and wildly ramified Galois extensions, Ann. Inst. Fourier, **41**, 1991, no.2, 393–430.
Burns,D. [95a]: On arithmetically realizable classes, Math. Proc. Cambridge Philos. Soc., **118**, 1995, 383–392.
Burns,D. [95b]: On multiplicative Galois structure invariants, Amer. J. Math., **117**, 1995, 875–903.
Burns,D.,Holland,D. [97]: Chinburg's third invariant for abelian extensions of imaginary quadratic fields, Proc. London Math. Soc., (3) **1974**, 29–51.
Bushnell,C.J. [77a]: Integrality of Galois Jacobi sums, J. London Math. Soc., (2) **15**, 1977, 35–40.
Bushnell,C.J. [77b]: Norms of normal integral generators, J. London Math. Soc., (2) **15**, 1977, 199–209.
Bushnell,C.J. [79]: Norm distribution in Galois orbits, J. Reine Angew. Math., **310**, 1979, 81–99.
Bushnell,C.J. [83]: Diophantine approximation and norm distribution in Galois orbits, Illinois J. Math., **27**, 1983, 145–157.
Bushnell,C.J.,Henniart,G. [01]: Sur le comportement, par torsion, des facteurs epsilon de paires, Canad. J. Math., **53**, 2001, 1141–1173.
Büsser,A.H. [44]: *Über die Primidealzerlegung in Relativkörpern mit der Relativgruppe* G_{168}, Diss. Univ. Zürich 1944.
Butts,H.S. [64]: Unique factorization of ideals into nonfactorable ideals, Proc. Amer. Math. Soc., **15**, 1964, p.21.
Butts,H.S.,Pall,G. [67]: Factorization in quadratic rings, Duke Math. J., **34**, 1967, 139–146.

Butts,H.S.,Pall,G. [68]: Modules and quadratic forms, Acta Arith., **15**, 1968, 23–44.
Butts,H.S.,Smith,W.W. [66]: On the integral closure of a domain, J. Sci. Hiroshima Univ., **30**, 1966, 117–122.
Butts,H.S.,Wade,L.I. [66]: Two criteria for Dedekind domains, Amer. Math. Monthly, **73**, 1966, 14–21.
Buzzard,K.,Dickinson,M.,Shepherd-Barron,N.,Taylor,R. [01]: On icosahedral Artin representations, Duke Math. J., **109**, 2001, 283–318.
Byeon,D. [96]: Class number one problem for pure cubic fields of Rudman-Stender type, Proc. Japan Acad. Sci., **72**, 1996, 166–167.
Byeon,D. [99a]: A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms, Acta Arith., **89**, 1999, 295–299.
Byeon,D. [99b]: Class numbers and Iwasawa invariants of certain totally real number fields, J. Number Theory, **79**, 1999, 249–257.
Byeon,D. [01a]: A note on class number 1 criteria for totally real algebraic number fields, Acta Arith., **100**, 2001, 291–295.
Byeon,D. [01b]: Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields, Compositio Math., **126**, 2001, 249–256.
Byeon,D.,Kim,H.K. [97]: Class number 2 criteria for real quadratic fields of Richaud-Degert type, J. Number Theory, **62**, 1997, 257–272.
Byeon,D.,Stark,H.M. [02]: On the finiteness of certain Rabinowitsch polynomials, J. Number Theory, **94**, 2002, 177–180; II, **99**, 2003, 219–221.
Byott,N.P.,Lettl,G. [96]: Relative Galois module structure of integers in abelian fields, J. Théor. Nombres Bordeaux, **8**, 1996, 125–141.
Cahen,P.-J., Chabert,J.-L. [95]: Elasticity for integral–valued polynomials, J. Pure Appl. Algebra, **103**, 1995, 303–311.
Callahan,T. [74]: The 3-class group of non-Galois fields, I, Mathematika, **21**, 1974, 72–89; II, 168–188.
Callahan,T. [76]: Dihedral field extensions of order $2p$ whose class numbers are multiples of p, Canad. J. Math., **28**, 1976, 429–439,
Callahan,T.,Newman,M.,Sheingorn,M. [77]: Fields with large Kronecker constants,I, J. Number Theory, **9**, 1977, 182–186.
Çallial,P.F. [80]: Non-nullité des fonctions zéta des corps quadratiques réels pour $0 < s < 1$, C.R. Acad. Sci. Paris, **291**, 1980, A623–625.
Calloway,J. [55]: On the discriminant of arbitrary algebraic number fields, Proc. Amer. Math. Soc., **6**, 1955, 482–489.
Cameron,P.J. [72]: On groups with several doubly transitive permutations, Math. Z., **128**, 1972, 1–14.
Camion,P.,Levy,L.S.,Mann,H.B. [73]: Prüfer rings, J. Number Theory, **5**, 1973, 132–138.
Canals,I.,Ortiz,J.J. [70]: The minimal basis of an algebraic number field, Bol. Soc. Mat. Mexicana, **16**, 1970, 14–21.
Candiotti,A. [74]: Computations of Iwasawa invariants and K_2, Compositio Math., **29**, 1974, 89–111.
Cantor,D.G. [65]: On the elementary theory of diophantine approximation over the ring of adeles, Illinois J. Math., **9**, 1965, 677–700.
Cantor,D.G. [76]: On certain algebraic integers and approximation by rational functions with integral coefficients, Pacific J. Math., **67**, 1976, 323–338.
Cantor,D.G. [80]: On an extension of the definition of transfinite diameter and some applications, J. Reine Angew. Math., **316**, 1980, 160–207.
Cantor,D.G.,Roquette,P. [84]: On Diophantine equations over the ring of all algebraic integers, J. Number Theory, **18**, 1984, 1–26.
Cantor,D.G.,Straus,E.G. [88]: On a conjecture of D.H.Lehmer, Acta Arith., **42**, 1988, 97–100; corr. p.325.

Carayol,H. [00]: Preuve de la conjecture de Langlands locale pour GL_n: travaux de Harris-Taylor et Henniart, Séminaire Bourbaki 1998/99, Astérisque, **266**, 2000, 191–243.
Carlitz,L. [33]: On abelian fields, Trans. Amer. Math. Soc., **35**, 1933, 122–136.
Carlitz,L. [52]: A note on common index divisors, Proc. Amer. Math. Soc., **3**, 1952, 688–692.
Carlitz,L. [53a]: The class number of an imaginary quadratic field, Comment. Math. Helv., **27**, 1953, 338–345.
Carlitz,L. [53b]: Note on the class number of real quadratic fields, Proc. Amer. Math. Soc., **4**, 1953, 535–537.
Carlitz,L. [53c]: A theorem of Stickelberger, Math. Scand., **1**, 1953, 82–84.
Carlitz,L. [54]: The first factor of the class number of a cyclic field, Canad. J. Math., **6**, 1954, 23–26.
Carlitz,L. [55]: Note on the class number of quadratic fields, Duke Math. J., **22**, 1955, 585–593.
Carlitz,L. [60]: A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc., **11**, 1960, 391–392.
Carlitz,L. [61]: A generalization of Maillet's determinant and a bound for the first factor of the class number, Proc. Amer. Math. Soc., **12**, 1961, 256–261.
Carlitz,L. [68]: A congruence for the second factor of the class number of a cyclotomic field, Acta Arith., **14**, 1968, 27–34; corr., **16**, 1970, p.437.
Carlitz,L.,Olson,F.R. [55]: Maillet's determinant, Proc. Amer. Math. Soc., **6**, 1955, 265–269.
Carroll,J.E.,Kisilevsky,H. [81]: On Iwasawa's λ-invariant for certain Z_l-extensions, Acta Arith., **40**, 1981, 1–8.
Carter,D.,Keller,G. [83]: Bounded elementary generation of $SL_n(\mathcal{O})$, Amer. J. Math., **105**, 1983, 673–687.
Carter,J.E. [96]: Steinitz classes of a nonabelian extension of degree p^3, Colloq. Math., **71**, 1996, 297–303.
Carter,J.E. [97]: Steinitz classes of nonabelian extensions of degree p^3, Acta Arith., **78**, 1997, 297–303.
Carter,J.E. [98]: Module structure of integers in metacyclic extensions, Colloq. Math., **76**, 1998, 191–199.
Carter,J.E. [99]: A generalization of a result on integers in metacyclic extensions, Colloq. Math., **81**, 1999, 153–156.
Cassels,J.W.S. [59a]: Note on quadratic forms over the rational field, Proc. Cambridge Philos. Soc., **55**, 1959, 267–270.
Cassels,J.W.S. [59b]: *An Introduction to the Geometry of Numbers*, Springer 1959.
Cassels,J.W.S. [66]: On a problem of Schinzel and Zassenhaus, J. Math. Sci., **1**, 1966, 1–8.
Cassels,J.W.S. [76]: An embedding theorem for fields, Bull. Austral. Math. Soc., **14**, 1976, 193–198; add.: 479–480.
Cassels,J.W.S. [86]: *Local Fields*, Cambridge 1986.
Cassels,J.W.S.,Fröhlich,A. (editors) [67]: *Algebraic Number Theory*, Academic Press 1967; reprint 1986.
Cassels,J.W.S.,Guy,M.J.T. [66]: On the Hasse principle for cubic surfaces, Mathematika, **13**, 1966, 111–120.
Cassels,J.W.S.,Wall,G.E. [50]: The normal basis theorem, J. London Math. Soc., **25**, 1950, 259–264.
Cassou-Noguès,P. [79]: Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques, Invent. math., **51**, 1979, 29–59.
Cassou-Noguès,P.,Fresnel,J. [79]: Le résidu des fonctions zêta de Shintani, Sém. Théor. Nombres Bordeaux, 1978/79, exp.2.

Cassou-Noguès,Ph. [77]: Quelques théorèmes de base normale, Astérisque, **41/42**, 1977, 183–189.

Cassou-Noguès,Ph. [78]: Quelques théorèmes de base normale d'entiers, Ann. Inst. Fourier, **28**, 1978, no.3, 1–33.

Cassou-Noguès,Ph.,Queyrut,J. [82]: Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées, Ann. Inst. Fourier, **32**. 1982, no.1, 7–27.

Cassou-Noguès,Ph.,Taylor,M. [87a]: *Elliptic Functions and Rings of Integers*, Birkhäuser 1987.

Cassou-Noguès,Ph.,Taylor,M. [87b]: Unités modulaires et monogènéité d'anneaux d'entiers, in: *Séminaire de Théorie des Nombres, Paris 1986-87*, 35–64. Birkhäuser 1987.

Cassou-Noguès,Ph.,Taylor,M. [88]: A note on elliptic curves and the monogeneity of rings of integers, J. London Math. Soc., (2) **37**, 1988, 63–72.

Cassou-Noguès,Ph.,Taylor,M. [91]: Un élément de Stickelberger quadratique, J. Number Theory, **37**, 1991, 307–342.

Cassou-Noguès,Ph.,Taylor,M. [00]: Galois module structure for wild extensions, in: *Algebraic Number Theory and Diophantine Analysis*, (Graz 1998), 69–91, de Gruyter 2000.

Castela,C. [78]: Nombre de classes d'idéaux d'une extension diédrale d'un corps de nombres, C.R. Acad. Sci. Paris, **287**, 1978, A483–486.

Cavallar,S.,Lemmermeyer,F. [98]: The Euclidean algorithm in cubic number fields, in: *Number Theory (Eger 1996)*, 123–146, de Gruyter 1998.

Cavallar,S.,Lemmermeyer,F. [00]: Euclidean windows, LMS J. Comput. Math., **3**, 2000, 336–355.

Cerri,J.P. [00]: De l'euclidianité de $Q(\sqrt{2+\sqrt{2+\sqrt{2}}})$ et $Q(\sqrt{2+\sqrt{2}})$, J. Théor. Nombres Bordeaux, **12**, 2000, 103–126.

Chabauty,C. [37]: Sur les unités d'un corps de nombres algébriques, qui sont sourmises à des conditions algébriques, C.R. Acad. Sci. Paris, **205**, 1937, 944–946.

Chabauty,C. [38]: Démonstration d'un théorème de Thue, indépendante de la théorie des approximations diophantiennes, C.R. Acad. Sci. Paris, **208**, 1938, 1196–1198.

Chamizo,F.,Iwaniec,H. [98]: On the Gauss mean-value theorem for class number, Nagoya Math. J.. **151**, 1998, 199–208.

Chan,S.-P.,Lim,C.-H. [93]: Relative Galois module structure of rings of integers of cyclotomic fields, J. Reine Angew. Math., **434**, 1993, 205–220.

Chan,S.-P.,Lim,C.-H. [95]: The associated order of rings of integers in Lubin-Tate division fields over the p-adic number field, Illinois J. Math., **39**, 1995, 30–38.

Chandrasekharan,K.,Good,A. [83]: On the number of integral ideals in Galois extensions, Monatsh. Math., **95**, 1983, 99–109.

Chandrasekharan,K.,Narasimhan,N. [62a]: Functional equation with multiple gamma factors and the average order of arithmetical functions, Ann. of Math., (2) **76**, 1962, 93–136.

Chandrasekharan,K.,Narasimhan,N. [62b]: The average order of arithmetical functions, and the approximate functional equation for a class of zeta-functions, Rend. Mat. Appl., (5) **21**, 1962, 354–363.

Chandrasekharan,K.,Narasimhan,N. [63]: The approximate functional equation for a class of zeta-functions, Math. Ann., **152**, 1963, 30–64.

Chandrasekharan,K.,Narasimhan,N. [64]: On the mean value of the error term for a class of arithmetical functions, Acta Math., **112**, 1964, 41–67.

Chandrasekharan,K.,Narasimhan,N. [68]: Zeta-functions of ideal classes in quadratic fields and their zeros on the critical line, Comment. Math. Helv., **43**, 1968, 18–30.

Chang,K.-Y.,Kwon,S.-H. [98]: Class number problems for imaginary cyclic number fields, J. Number Theory, **73**, 1998, 318–338.

Chang,K.-Y.,Kwon,S.-H. [00a]: Class numbers of imaginary abelian fields, Proc. Amer. Math. Soc., **128**, 2000, 2517–2528.
Chang,K.-Y.,Kwon,S.-H. [00b]: The imaginary abelian number fields with class number equal to their genus class numbers, J. Théor. Nombres Bordeaux, **12**, 2000, 249–365.
Chang,K.-Y.,Kwon,S.-H. [02]: The non-abelian normal CM-fields of degree 36 with class number one, Acta Arith., **101**, 2002, 53–61.
Chang,K.-Y.,Kwon,S.-H. [03]: The class number one problem for some non-abelian normal CM-fields of degree 48, Math. Comp., **72**, 2003, 1003–1017.
Chang,M.L. [02]: Non-monogeneity in a family of sextic fields, J. Number Theory, **97**, 2002, 252–268.
Chang,S.M. [77]: *Capitulation Problem in Algebraic Number Fields*, Ph.D. thesis, Univ. Toronto 1977.
Chang,S.M.,Foote,R. [80]: Capitulation in class field extensions of type (p, p), Canad. J. Math., **32**, 1980, 1229–1243.
Chao,N.L. [51]: Discrete-valued complete fields with residue class fields of characteristic p, J. Chinese Math. Soc., **1**, 1951, 377–394.
Chapman,R.J.. [96]: A simple proof of Noether's theorem, Glasgow Math. J., **38**, 1996, 49–51.
Chapman,S.T. [95]: On the Davenport constant, the cross number, and their application in factorization theory, in: *Zero-dimensional Commutative Rings*, Lecture Notes in Pure and Appl. Math., **171**, 167–190, Marcel Dekker 1995.
Chapman,S.T.,Coykendall,J. [00]: Half-factorial domains, a survey, in: *Non-Noetherian Commutative Ring Theory*, 97–115, Kluwer 2000.
Chapman,S.,Geroldinger,A. [97]: Krull domains and monoids, their sets of lengths, and associated combinatorial problems, in: *Factorization in Integral Domains*, Lecture Notes in Pure and Appl. Math., **189**, 73–112, Marcel Dekker 1997.
Chapman,S.T.,Herr,J.,Rooney,N. [99]: A factorization formula for class number two, J. Number Theory, **79**, 1999, 58–66.
Chapman,S.T.,Smith,W.W. [90a]: Factorization in Dedekind domains with finite class group, Israel J. Math., **71**, 1990. 391–392.
Chapman,S.T.,Smith,W.W. [90b]: On a characterization of algebraic number fields with class number less than three, J. Algebra, **135**, 1990, 381–387.
Chapman,S.T.,Smith,W.W. [92a]: On the HFD, CHFD and k-HFD properties in Dedekind domains, Comm. Algebra, **20**, 1992, 1955–1987.
Chapman,S.T.,Smith,W.W. [92b]: On the k-HFD property in Dedekind domains with small class groups, Mathematika, **39**, 1992, 330–340.
Chapman,S.T.,Smith,W.W. [93a]: On the lengths of factorizations of elements in an algebraic number ring, J. Number Theory, **43**, 1993, 24–30.
Chapman,S.T.,Smith,W.W. [93b]: An analysis using the Zaks-Skula constant of element factorizations in Dedekind domains, J. Algebra, **159**, 1993, 176–190.
Chapman,S.T.,Smith,W.W. [98]: Generalized sets of lengths, J. Algebra, **200**, 1998, 449–471.
Chatelain,D. [70]: Bases normales de l'anneau des entiers de certaines extensions abéliennes, de Q, C.R. Acad. Sci. Paris. **270**, 1970, A557–560.
Chatelain,D. [73]: Bases des entiers des corps composés par des extensions quadratiques, Ann. Univ. Besançon, Math., 1973, fasc.6.
Châtelet,A. [11]: Sur certains ensembles des tableaux et leur application à la théorie des nombres, Ann. Sci. École Norm. Sup., (2) **28**, 1911, 105–202.
Châtelet,A. [46]: Arithmétique des corps abéliens du troisième degré, Ann. Sci. École Norm. Sup., (2) **63**, 1946, 109–160.
Chatland,H.,Davenport,H. [50]: Euclid's algorithm in real quadratic fields, Canad. J. Math., **2**, 1950, 289–296.

Chebotarev,N.G. [23a]: On a theorem of Hilbert, Visti VUAN, 1923, 3–7. (Russian)
Chebotarev,N.G. [23b]: Determination of the density of the set of primes corresponding to a given class of permutations, Izv. Akad. Nauk SSSR, Ser. Mat., **17**, 1923, 205–230, 231–250. (Russian)
Chebotarev,N.G. [24]: Proof of the Kronecker-Weber theorem on Abelian fields, Mat. Sb., **31**, 1924, 302–309. (Russian)
Chebotarev,N.G. [26]: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebener Substitutionsklasse gehören, Math. Ann., **95**, 1926, 191–228.
Chebotarev,N.G. [29]: Zur Gruppentheorie des Klassenkörpers, J. Reine Angew. Math., **161**, 1929, 179–193; corr.: **164**, 1931, p.196.
Chebotarev,N.G. [30]: The foundation of the ideal theory of Zolotarev, Amer. Math. Monthly, **37**, 1930, 117–118.
Chebotarev,N.G. [37a]: *Foundations of the Galois Theory*, II, Moskva-Leningrad 1937. (Russian)
Chebotarev,N.G. [37b]: Kurzer Beweis des Diskriminantensatzes, Acta Arith., **1**, 1937, 78–82.
Chebotarev,N.G. [37c]: Eine Aufgabe aus der algebraischen Zahlentheorie, Acta Arith., **2**, 1937, 221–229.
Chebotarev,N.G. [47]: On the foundations of the ideal theory, Uspekhi Mat. Nauk, **2**, 1947, nr.6, 52–67. (Russian)
Chen,Y.-M.J.,Kitaoka,Y.,Yu,J. [00]: Distribution of units of real quadratic number fields, Nagoya Math. J., **158**, 2000, 167–184.
Cherubini,J.M.,Wallisser,R.V. [87]: On the computation of all imaginary quadratic fields of class number one, Math. Comp., **49**, 1987, 295–299.
Chevalley,C. [31]: Relation entre le nombre de classes d'un sous-corps et celui d'un surcorps, C.R. Acad. Sci. Paris, **192**, 1931, 257–258.
Chevalley,C. [33]: Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sci. Univ. Tokyo, **2**, 1933, 365–476.
Chevalley,C. [36a]: Généralisation de la théorie du corps de classes pour les extensions infinies, J. math. pures appl., (9) **15**, 1936, 359–371.
Chevalley,C. [36b]: *L'arithmétique sur les algèbres de matrices*, Hermann 1936.
Chevalley,C. [40]: La théorie du corps de classes, Ann. of Math., (2) **41**, 1940, 394–418.
Chevalley,C. [54]: *Class Field Theory*, Nagoya 1954.
Childs,L.N. [77]: The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc., (3) **35**, 1977, 407–422.
Childs,L.N. [80]: Stickelberger relations on tame Kummer extensions of prime degree, in: *Proc. Queen's Number Theory Conference 1979*, 249–256, Kingston 1980.
Childs,L.N. [81]: Stickelberger relations and tame extensions of prime degree, Illinois J. Math., **25**, 1981, 258–266.
Chinburg,T. [83a]: Stark's conjecture for L-functions with first order zeroes at $s = 0$, Adv. in Math., **48**, 1983, 82–113.
Chinburg,T. [83b]: On the Galois structure of algebraic integers and S-units, Invent. math., **74**, 1983, 321–349.
Chinburg,T. [83c]: Derivatives of L-functions at $s = 0$, Compositio Math., **48**, 1983, 119–127.
Chinburg,T. [84]: Multiplicative Galois module structure, J. London Math. Soc., (2) **29**, 1984, 23–33.
Chinburg,T. [85]: Exact sequences and Galois module structure, Ann. of Math., (2) **121**, 1985, 351–376.
Chinburg,T. [89]: The analytic theory of multiplicative Galois structure, Mem. Amer. Math. Soc., **77**, 1989, 1–158.

Chinburg,T. [91]: Capacity theory on varieties, Compositio Math., **80**, 1991, 75–84.
Chowla,P. [68]: On the class-number of real quadratic fields, J. Reine Angew. Math., **230**, 1968, 51–60.
Chowla,P. [74]: On the non-vanishing of a certain L-series at $s = 1/2$, J. Number Theory, **6**, 1974, 158–159.
Chowla,P.,Chowla,S. [68]: Formulae for the units and class-numbers of real quadratic fields, J. Reine Angew. Math., **230**, 1968, 61–65.
Chowla,P.,Chowla,S. [72]: Problems on periodic simple continued fractions, Proc. Nat. Acad. Sci. U.S.A., **69**, 1972, p.3745.
Chowla,P.,Chowla,S. [73]: On Hirzebruch sums and a theorem of Schinzel, Acta Arith., **24**, 1973, 223–224.
Chowla,S. [34a]: The class-number of binary quadratic forms, Quart. J. Math., Oxford ser., **5**, 1934, 302–303.
Chowla,S. [34b]: An extension of Heilbronn's class-number theorem, Quart. J. Math., Oxford ser., **5**, 1934, 304–307.
Chowla,S. [34c]: On the k-analogue of a result in the theory of the Riemann zeta function, Math. Z., **38**, 1934, 483–487.
Chowla,S. [34d]: Heilbronn's class-number theorem, I, J. Indian Math. Soc., **1**, 1934, 66–68; II, Proc. Nat. Acad. Sci. India, A, **1**, 1934, 145–146.
Chowla,S. [36]: Note on Dirichlet's L-functions, Acta Arith., **1**, 1936, 113–114.
Chowla,S. [50]: A new proof of a theorem of Siegel, Ann. of Math., (2) **51**, 1950, 120–122.
Chowla,S. [61a]: Proof of a conjecture of Julia Robinson, Norske Vid. Selsk. Forh., **34**, 1961, 100–101.
Chowla,S. [61b]: A remarkable solution of the Pellian equation $X^2 - pY^2 = -4$ in the case when $p \equiv 1 \pmod 4$ and the class-number of $R(\sqrt{p})$ is 1, J. Indian Math. Soc., **25**, 1961, 43–46.
Chowla,S. [62]: On Gaussian sums, Norske Vid. Selsk. Forh., **35**, 1962, 66–67.
Chowla,S. [64]: Bounds for the fundamental unit of a real quadratic field, Norske Vid. Selsk. Forh., **37**, 1964, 88–90.
Chowla,S. [70a]: The Heegner-Stark-Baker-Deuring-Siegel theorem, J. Reine Angew. Math., **241**, 1970, 47–48.
Chowla,S. [70b]: Leopoldt's criterion for real quadratic fields with class-number 1, Abh. Math. Sem. Univ. Hamburg, **35**, 1970, p.32.
Chowla,S.,Briggs,W.E. [54]: On discriminants of binary quadratic forms with a single class in each genus, Canad. J. Math., **6**, 1954, 463–470.
Chowla,S.,Cowles,M. [77]: On the coefficients c_n in the expansion

$$x\prod_1^\infty (1-x^n)^2(1-x^{11n})^2 = \sum_1^\infty c_n x^n,$$

J. Reine Angew. Math., **292**, 1977, 115–116.
Chowla,S.,Erdős,P. [51]: A theorem on the distribution of the values of L-functions, J. Indian Math. Soc., **15**, 1951, 11–18.
Chowla,S.,Friedlander,J.B. [76a]: Class numbers and quadratic residues, Glasgow Math. J., **17**, 1976, 47–52.
Chowla,S.,Friedlander,J.B. [76b]: Some remarks on L-functions and the class numbers, Acta Arith., **28**, 1976, 413–417.
Chowla,S.,Goldfeld,D.M. [76]: A remark on certain Hecke L-series which are non-negative on the real axis, Acta Arith., **30**, 1976, 1–3.
Chowla,S.,Hartung,P. [74a]: Congruence properties of class numbers of quadratic fields, J. Number Theory, **6**, 1974, 136–137.

Chowla,S.,Hartung,P. [74b]: A note on the hypothesis that $L(s,\chi) > 0$ for all real non-principal characters χ and for all $s > 0$, J. Number Theory, **6**, 1974, 271–275.
Chowla,S.,Kessler,I.,Livingston.M. [77]: On character sums and non-vanishing of Dirichlet's L-series belonging to real odd characters χ, Acta Arith., **33**, 1977, 81–87.
Chowla,S.,de Leon,M.J. [74]: A note on the Hecke hypothesis and the determination of imaginary quadratic fields with class-number 1, J. Number Theory, **6**, 1974, 261–263.
Chowla,S.,de Leon,M.J.,Hartung,P. [73]: On a hypothesis implying the non-vanishing of Dirichlet's L-series $L(s,\chi)$ for $s > 0$ and real odd characters. J. Reine Angew. Math., **262/263**, 1973, 415–419.
Chowla,S.,Vijayaraghavan,T. [44]: The complete factorization (mod p) of the cyclotomic polynomial of order $p^2 - 1$, Proc. Nat. Acad. Sci. India, A, **14**, 1944, 101–105.
Christofferson,S. [57]: Über eine Klasse von kubischen Gleichungen mit drei Unbekannten, Ark. Mat., **3**, 1957, 355–364.
Chudakov,N.G. [42]: On Siegel's theorem, Izv. Akad. Nauk SSSR, Ser. Mat., **6**, 1942, 135–142. (Russian)
Chudakov,N.G. [69]: Upper bound for the discriminant of the tenth imaginary quadratic field with class number one, Issled. Teor. Chisel, Saratov, **3**, 1969, 75–77. (Russian)
Chulanovskii,I.V. [56]: Elementary proof of the law of distribution of primes in the Gaussian field, Vestnik LGU, **11**, 1956, no.13, 43–62.
Cioffari,V.G. [79]: The euclidean condition in pure cubic and complex quartic fields, Math. Comp., **33**. 1979, 389–398.
Claborn,L. [65]: Dedekind domains and rings of quotients, Pacific J. Math., **15**, 1965, 59–64.
Claborn,L. [66]: Every abelian group is a class group, Pacific J. Math., **18**, 1966, 219–222.
Claborn,L. [68]: Specified relations in the ideal group, Michigan J. Math., **15**, 1968, 249–255.
Claborn,L.,Fossum,R. [68]: Generalizations of the notion of class-group, Illinois J. Math., **12**, 1968, 228–253.
Clark,D.A. [94]: A quadratic field which is Euclidean but not norm-Euclidean, Manuscripta Math., **83**, 1994, 327–330.
Clark,D.A. [96]: Non-Galois cubic fields which are Euclidean but not norm-Euclidean, Math. Comp., **65**, 1996, 1675–1679.
Clark,D.A.,Murty,M.R. [95]: The Euclidean algorithm for Galois extensions of Q, J. Reine Angew. Math., **459**, 1995, 151–162.
Coates,J. [77]: p-adic L-functions and Iwasawa's theory, in: *Algebraic Number Fields*, 269–353, Academic Press 1977.
Coates,J. [81]: The work of Mazur and Wiles on cyclotomic fields, in: *Seminaire Bourbaki 1980/81*, Lecture Notes in Math., **901**, 220–242, Springer 1981.
Coates,J. [86]: The work of Gross and Zagier on Heegner points and the derivatives of L-series, Astérisque, **133/134**, 57–72, 1986.
Coates,J.,Lichtenbaum,S. [73]: On l-adic zeta functions, Ann. of Math., (2) **98**, 1973, 498–550.
Coates,J.,Sinnott,W. [77]: Integrality properties of the values of partial zeta functions, Proc. London Math. Soc., (3) **34**, 1977, 365–384.
Coates,J.,Wiles,A. [77]: Kummer's criterion for Hurwitz numbers, in: *Algebraic Number Theory, Kyoto*, 9–23, Tokyo 1977.
Coates,J.,Wiles,A. [78]: On p-adic L-functions and elliptic units, J. Austral. Math. Soc., **26**, 1978, 1–25.

Cohen,G.L. [75a]: Boundary conditions for expanding domains, Acta Arith., **26**, 197, 213–216.
Cohen,G.L. [75b]: Selberg formulae for Gaussian integers, Acta Arith., **26**, 1975, 385–400.
Cohen,H. [74]: Variations sur un thème de Siegel-Hecke, Publ. Math. Un. Bordeaux, 1973/74, no.5, 1–45.
Cohen,H. [76]: Variations sur un thème de Siegel et Hecke, Acta Arith., **30**, 1976, 63–93.
Cohen,H. [83]: Sur la distribution asymptotique des groupes de classes, C.R. Acad. Sci. Paris, **296**, 1983, 245–247.
Cohen,H. [93]: *A Course in Computational Algebraic Number Theory*, Springer 1993.
Cohen,H. [00a]: *Advanced Topics in Computational Number Theory*, Springer 2000.
Cohen,H. [00b]: Comptage exact de discriminants d'extensions abéliennes, J. Théor. Nombres Bordeaux, **12**, 2000, 379–397.
Cohen,H. [02]: Constructing and counting number fields, in: *Proceedings of the ICM 2002, (Beijing)*, **II**, 129–138, Beijing 2002.
Cohen,H. [03]: Enumerating quartic dihedral extensions of $\mathbb{Q}$ with signatures, Ann. Inst. Fourier, **53**, 2003, no.2, 339–377.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [98a]: Computing ray class groups, conductors and discriminants, Math. Comp., **67**, 1998, 773–795.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [98b]: A table of totally complex number fields of small discriminants, in: *Algorithmic Number Theory (Portland 1998)*, 381–391.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [99]: Tables of octic fields with a quartic subfield, Math. Comp., **68**, 1999, 1701–1716.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [00]: Counting discriminants of number fields of degree up to four, in *Algorithmic Number Theory (Leiden 2000)*, 269–283, Lecture Notes in Comput. Sci., **1838**, Springer 2000.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [02a]: On the density of discriminants of cyclic extensions of prime degree, J. Reine Angew. Math., **550**, 2002, 169–209.
Cohen,H.,Diaz y Diaz,F.,Olivier,M. [02b]: Enumerating quartic dihedral extensions of Q, Compositio Math., **133**, 2002, 65–93.
Cohen,H.,Lenstra,H,W,Jr, [84]: Heuristic on class group of number fields, in: *Number Theory, Noordwijkerhout 1983*, 33–62, Lecture Notes in Math., **1068**, Springer 1984.
Cohen,H.,Martinet,J. [87]: Class groups of number fields: numerical heuristics, Math. Comp., **48**, 1987, 123–137.
Cohen,H.,Martinet,J. [90]: Étude heuristique des groupes de classes des corps de nombres, J. Reine Angew. Math., **404**, 1990, 39–76.
Cohen,H.,Martinet,J. [94]: Heuristics on class groups: some good primes are not too good, Math. Comp., **63**, 1994, 329–334.
Cohen,I.S. [50]: Commutative rings with restricted minimum condition, Duke Math. J., **17**, 1950, 27–42.
Cohn,H. [54]: The density of abelian cubic fields, Proc. Amer. Math. Soc., **5**, 1954, 476–477.
Cohn,H. [56a]: A device for generating fields of even class numbers, Proc. Amer. Math. Soc., **7**, 1956, 595–598.
Cohn,H. [56b]: Some algebraic number theory estimates based on Dedekind Eta-functions, Amer. J. Math., **78**, 1956, 791–796.
Cohn,H. [60]: A numerical study of Weber's real class number calculation, Numer. Math., **2**, 1960, 347–362.
Cohn,H. [76]: Dyadotropic polynomials, Math. Comp., **30**, 1976, 854–862; II, **39**, 1979, 359–367.

Cohn,H. [78]: *A Classical Introduction to Algebraic Numbers and Class Fields*, Springer 1978.
Cohn,H. [79a]: Quaternionic compositum genus, J. Number Theory, **11**, 1979, 399–411.
Cohn,H. [79b]: Cyclic-sixteen class fields for $Q((-p)^{1/2})$ by modular arithmetic, Math. Comp., **33**, 1979, 1307–1316.
Cohn,H. [81a]: The explicit Hilbert 2-cyclic class field for $Q(\sqrt{-p})$, J. Reine Angew. Math., **321**, 1981, 64–77.
Cohn,H. [81b]: Iterated ring class fields and the icosahedron, Math. Ann., **255**, 1981, 107–122.
Cohn,H. [83]: Some examples of Weber-Hecke ring class field theory, Math. Ann., **265**, 1983, 83–100.
Cohn,H. [85]: *Introduction to the Construction of Class Fields*, Cambridge 1985. [Reprint: Dover 1994.]
Cohn,H.,Cooke,G.E. [76]: Parametric form of an eight class field, Acta Arith.. **30**, 1976, 367–377.
Cohn,H.,Lagarias,J.C. [83]: On the existence of fields governing the 2-invariants of the class-group of $\mathbb{Q}(\sqrt{dp})$ as p varies, Math. Comp., **41**, 1983, 711–730.
Cohn,J.H.E. [77]: The length of the period of the simple continued fraction of $\sqrt{d}$, Pacific J. Math., **71**, 1977, 21–32.
Coleman,M.D. [90]: A zero-free region for the Hecke L-functions, Mathematika, **37**, 1990, 287–304.
Coleman,M.D. [93]: The Rosser-Iwaniec sieve in number fields, with an application, Acta Arith., **65**, 1993, 53–83.
Coleman,M.D. [98]: The normal density of prime ideals in small region, Monatsh. Math., **125**, 1998, 111–126.
Coleman,R.F.,McCallum,W.G. [88]: Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. Reine Angew. Math., **385**, 1988, 41–101.
Colliot-Thélène,J.-L.,Coray,D.,Sansuc,J.J. [80]: Descente et principe de Hasse pour certaines variétés rationnelles, J. Reine Angew. Math., **320**, 1980, 150–191.
Colliot-Thélène,J.-L.,Sansuc,J.J. [82]: Sur le principe de Hasse et l'approximation faible, et sur une hypothése de Schinzel, Acta Arith., **41**, 1982, 33–53.
Colmez,P. [88]: Résidu en $s = 1$ des fonctions zêta p-adiques, Invent. math., **91**, 1988, 371–389.
Colmez,P. [00]: Fonctions L p-adiques, Séminaire Bourbaki 1998/99, Astérisque, **266**, 2000, 21–58.
Connell,I.G. [62]: On algebraic number fields with unique factorization, Canad. Math. Bull., **5**, 1962, 151–156.
Connell,I.G.,Sussman,D. [70]: The p-dimension of class-groups of number fields, J. London Math. Soc., (2) **2**, 1970, 525–529.
Conner,P.E.,Perlis,R. [84]: *Survey of Trace Forms in Algebraic Number Fields*, World Scientific 1984.
Conrad,M.,Replogle,D.R. [03]: Nontrivial Galois module structure of cyclotomic fields, Math. Comp., **72**, 2003, 891–899.
Conrey,J.B.,Ghosh,A. [93]: On the Selberg class of Dirichlet series: small degrees, Duke Math. J., **72**, 1993, 673–693.
Conrey,J.B.,Ghosh,A.,Gonek,S.M. [86]: Simple zeros of the zeta function of a quadratic number field, I. Invent. math., **86**, 1986, 563–576; II, in: *Analytic Number Theory and Diophantine Problems (Stillwater, 1984)*, 87–114, Progr. Math., **70**, Birkhäuser 1987.
Conrey,[J].B.,Iwaniec,H. [02]: Spacing of zeros of Hecke L-functions and the class number problem, Acta Arith., **103**, 2002, 259–312.

Conrey,J.B.,Soundararajan,K. [02]: Real zeros of quadratic Dirichlet functions, Invent. math., **150**, 2002, 1–44.
Conway,J.H.,Jones,A.J. [76]: Trigonometric diophantine equations (On vanishing sums of roots of unity), Acta Arith., **30**, 1976, 229–240.
Cooke,G.E. [76]: A weakening of the euclidean property for integral domains and application to algebraic number theory, I, J. Reine Angew. Math., **282**, 1976, 133–156.
Cooke,G.E.,Weinberger,P.J. [75]: On the construction of division chains in algebraic number rings, with applications to SL_2, Comm. Algebra, **3**, 1975, 481–524.
Coolidge,J.L. [08]: The continuity of roots of an algebraic equation, Ann. of Math., (2) **9**, 1908, 116–118.
Cornacchia,P. [97]: The parity of the class number of the cyclotomic fields of prime conductor, Proc. Amer. Math. Soc., **125**, 1997, 3163–3168.
Cornacchia,P. [01]: The 2-ideal class groups of $\mathbb{Q}(\zeta_l)$, Nagoya Math. J., **162**, 2001, 1–18.
Cornell,G. [71]: Abhyankar's lemma and the class group, in: *Number Theory, Carbondale 1977*, 82–88, Lecture Notes in Math., **751**, Springer 1971.
Cornell,G. [83a]: Exponential growth of the l-rank of the class group of the maximal real subfield of cyclotomic fields, Bull. Amer. Math. Soc., (N.S.) **8**, 1983, 55–58.
Cornell,G. [83b]: Relative genus theory and the class group of l-extensions, Trans. Amer. Math. Soc., **277**, 1983, 421–429.
Cornell,G.,Rosen,M. [81]: Group-theoretic constraints on the structure of the class group, J. Number Theory, **13**, 1981, 1–11.
Cornell,G.,Rosen,M. [84]: The l-rank of the real class-group of cyclotomic fields, J. Number Theory, **21**, 1985, 260–274.
Cornell,G., Washington,L. [85]: Class numbers of cyclotomic fields, J. Number Theory, **21**, 1985, 260–274.
Corput,J.G.van der [23]: Neue zahlentheoretische Untersuchungen, Math. Ann., **89**, 1923, 215–254.
Costa,A. [93]: A generalization of a result of Barrucand and Cohn on class numbers, J. Number Theory, **45**, 1993, 254–260.
Costa,A.,Friedman,E. [93]: Ratios of regulators in extensions of number fields, Proc. Amer. Math. Soc., **119**, 1993, 381–390.
Costa,A.,Gerth,F.III [95]: Densities for 4-class ranks of totally complex quadratic extensions of real quadratic fields, J. Number Theory, **54**, 1995, 274–286.
Cougnard,J. [72]: Sur les extensions galoisiennes non abéliennes de degré pq (p et q premiers) de rationnels, C.R. Acad. Sci. Paris, **274**, 1972, 936–939.
Cougnard,J. [73]: Sur l'anneau des entiers des extensions galoisiennes à groupe de Galois quaternionien d'ordre $4p$, Publ. Math. Univ. Bordeaux, 1973/74. no.1, 1–21.
Cougnard,J. [74]: Sur l'anneau des entiers des extensions galoisiennes non abéliennes de degré pq des rationnels, Bull. Soc. Math. France, Mém. **37**, 1974, 33–34.
Cougnard,J. [75]: Sur l'anneau des entiers des p-extensions, Astérisque, **24/25**, 1975, 15–20.
Cougnard,J. [76]: Propriétés galoisiennes des anneaux entiers des p-extensions, Compositio Math., **33**, 1976, 303–336.
Cougnard,J. [77]: Un contre-exemple à une conjecture de Martinet, in: *Algebraic Number Fields*, 539–560, Academic Press 1977.
Cougnard,J. [80]: Une propriété des entiers des extensions galoisiennes non abéliennes de degré pq des rationnels, Compositio Math., **40**, 1980, 407–415.
Cougnard,J. [82]: Propriétés locales et globales de certaines extensions métacycliques, Ann. Inst. Fourier, **32**, 1982, no.2, 1–12.

Cougnard,J. [83a]: Une remarque sur l'anneau des entiers du corps des racines septiemes de l'unité, Publ. Math. Fac. Sci. Besançon, 1981/82 et 1982/83.
Cougnard,J. [83b]: Les travaux de A.Fröhlich, Ph.Cassou-Noguès et M.J.Taylor sur les bases normales, *Séminaire Bourbaki*, **35**, 1982/83, exp.598, Astérisque, **105/106**, 25–38.
Cougnard,J. [85]: Quelques extensions modérément ramifiées sans base normale, J. London Math. Soc., (2) **31**, 1985, 200–204.
Cougnard,J. [86]: Bases normales relatives dans certains extensions cyclotomiques, J. Number Theory, **23**, 1986, 336–346.
Cougnard,J. [87a]: Sur la monogènéité de l'anneaux des entiers d'une extension diédrale imaginaire de degré $2p$ (p premier), Archiv Math., **48**, 1987, 223–231.
Cougnard,J. [87b]: Monogénéité de l'anneaux des entiers des extensions cycliques imaginaires de degré $2l$ (l premier ≥ 5), J. Reine Angew. Math., **375/376**, 1987, 42–46.
Cougnard,J. [88]: Conditions necessaires de monogénéité. Application aux extensions cycliques de degré premier $l \geq 5$ d'un corps quadratique imaginaire, J. London Math. Soc., (2) **37**, 1988, 73–87.
Cougnard,J. [90]: Modéle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers,I, Acta Arith., **54**, 1990, 191–212; II, **55**, 1990, 75–81.
Cougnard,J. [94]: Un anneau stablement libre et non libre, Experiment Math., **3**, 1994, 129–136.
Cougnard,J. [00]: Construction de base normale pour les extensions de Q à groupe D_4, J. Théor. Nombres Bordeaux, **12**, 2000, 399–409.
Cougnard,J.,Fleckinger,B. [89]: Sur la monogénéité de l'anneau des entiers de certains corps de rayon, Manuscripta Math., **63**, 1989, 365–376.
Cougnard,J.,Queyrut,J. [02]: Construction de bases normales pour les extensions galoisiennes absolues à groupe de Galois quaternionien d'ordre 12, J. Théor. Nombres Bordeaux, **14**, 2002, 87–102.
Cougnard,J.,Verant,M. [92]: Monogénéité de l'anneau des entiers de corps de rayon de corps quadratiques, Sém. Théor. Nombres Bordeaux, (2) **4**, 1992, 53–74.
Cowles,M.J. [80]: On the divisibility of the class number of imaginary quadratic fields, J. Number Theory, **12**, 1980, 113–115.
Coykendall,J. [96]: Normsets and determination of unique factorization in rings of algebraic integers, Proc. Amer. Math. Soc., **124**, 1996, 1727–1732.
Coykendall,J. [99]: The half-factorial property in integral extensions, Comm. Algebra, **27**, 1999, 3153–3159,
Coykendall,J. [00]: A remark on arithmetical equivalence and the normset, Acta Arith., **92**, 2000, 105–108.
Coykendall,J. [01]: Half-factorial domains in quadratic fields, J. Algebra, **235**, 2001, 417–430.
Craig,M. [77]: A construction for irregular discriminants, Osaka Math. J., **14**, 1977, 365–402; corr., **15**, 1978, p.461.
Cremona,J.E.,Odoni,R.W.K. [90]: A generalization of a result of Iwasawa on the capitulation problem, Math. Proc. Cambridge Philos. Soc., **107**, 1990, 1–3.
Cucker,F.,Corbalan,A.G. [89]: An alternate proof of the continuity of the roots of a polynomial, Amer. Math. Monthly, **96**, 1989, 342–345.
Cuoco,A.A. [80]: The growth of Iwasawa invariants in a family, Compositio Math., **41**, 1980, 415–437.
Cuoco,A.A. [82]: Relations between invariants in Z_p^2-extensions, Math. Z., **181**, 1982, 197–200.
Cuoco,A.A. [84]: Generalized Iwasawa invariants in a family, Compositio Math., **51**, 1984, 89–103.

Cuoco,A.A.,Monsky.P. [81]: Class numbers in Z_p^d-extensions, Math. Ann., **255**, 1981, 253–258.
Cusick,T.W. [82]: Finding fundamental units in cubic fields, Math. Proc. Cambridge Philos. Soc., **92**, 1982, 385–389.
Cusick,T.W. [84a]: Lower bounds for regulators, Lecture Notes in Math., **1068**, 63–73, Springer 1984.
Cusick,T.W. [84b]: Finding fundamental units in totally real fields, Math. Proc. Cambridge Philos. Soc., **96**, 1984, 191–194.
Cvetkov,V.M. [83]: On the Stickelberger-Voronoi theorem, Zap. Nauchn. Sem. LOMI, **103**, 1980, 146–149. (Russian)
Czarnowski,R. [82]: On the zeros of Dedekind zeta-function on the line $\sigma = 1/2$, Funct. Approx. Comment. Math., **13**, 1982, 149–154.
Czogała,A. [81]: Arithmetic characterization of algebraic number fields with small class numbers, Math. Z., **176**, 1981, 247–253.
Daberkow,M.,Pohst,M. [98]: On the computation of Hilbert class fields, J. Number Theory, **69**, 1998, 213–230.
Dade,E.C. [63]: Algebraic integral representations by arbitrary forms, Mathematika, **10**, 1963, 96–100; corr.: **11**, 1964, 89–90; addendum: **28**, 1981, p.87.
Dalen,K. [55]: On a theorem of Stickelberger, Math. Scand., **3**, 1955, 124–126.
Damey,P.,Payan,J.J. [70]: Existence et construction des extensions galoisiennes et nonabéliennes de degré 8 d'un corps de caractéristique differente de 2, J. Reine Angew. Math., **244**, 1970, 37–54.
Daniel,S.,Fouvry,E. [99]: On real quadratic fields with odd class number, Math. Ann., **313**, 1999, 371–384.
Datskovsky,B.A. [93]: A mean-value theorem for class numbers of quadratic extensions, in: *A Tribute to Emil Grosswald: Number Theory and Related Analysis*, Contemp. Math., **143**, 179–242.
Datskovsky,B.,Wright,D.J. [88]: Density of discriminants of cubic extensions, J. Reine Angew. Math., **386**, 1988, 116–138.
Davenport,H. [49]: Sur les corps cubiques à discriminants négatifs, C.R. Acad. Sci. Paris, **228**, 1949, 883–885.
Davenport,H. [50a]: Euclid's algorithm in cubic fields of negative discriminant, Acta Math., **84**, 1950, 159–179.
Davenport,H. [50b]: Euclid's algorithm in certain quartic fields , Trans. Amer. Math. Soc., **68**, 1950, 508–532.
Davenport,H. [52]: Linear forms associated with an algebraic number field, Quart. J. Math., Oxford ser., (2) **3**, 1952, 32–41.
Davenport,H.,Hasse,H. [34]: Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math., **172**, 1934, 151–182.
Davenport,H.,Heilbronn,H. [69]: On the density of discriminants of cubic fields, Bull. London Math. Soc., (2), **1** 1969, 345–348; II, Proc. Roy. Soc. London, A, **322**, 1971, 405–420.
David,P. [78]: Détermination de la structure des unités principales d'une extension abélienne K d'un corps local régulier, considéré comme un $Z_p(G(K/k))$-module, C.R. Acad. Sci. Paris, **286**, 1978, A985–986.
Davis,H.T. [35]: *Tables of Higher Mathematical Functions*, Bloomington 1935.
Davis,R.W. [76]: Class number formulae for imaginary quadratic fields, J. Reine Angew. Math., **286/287**, 1976, 369–379; II, **299/300**, 247–255.
Debarre,O.,Klassen,M. [94]: Points of low degree on smooth plane curves, J. Reine Angew. Math., **446**, 1994, 81–87.
Decomps-Guilloux,A. [65a]: Ensembles d'éléments algébriques dans les adèles, C.R. Acad. Sci. Paris, **261**, 1965, 1929–1931.

Decomps-Guilloux,A. [65b]: Ensembles d'éléments définis dans les adèles comme limite de certaines suites de rationelles, C.R. Acad. Sci. Paris, **261**, 1965, 3925–3926.

Decomps-Guilloux,A. [70]: Généralisations des nombres de Salem aux adèles, Acta Arith., **16**, 1970, 265–314.

Dedekind,R. [57]: Beweis für die Irreduktibilität der Kreisteilungs-Gleichungen, J. Reine Angew. Math., **54**, 1857, 27–30 = *Gesammelte mathematische Werke*, **I**, 68–71, Vieweg, 1930.

Dedekind,R. [71]: Über die Theorie der ganzen algebraischen Zahlen, XI Supplement to Dirichlet's " *Vorlesungen über Zahlentheorie*"; 2nd ed. 1871, 3rd ed. 1879, 4th ed. 1894 = *Gesammelte mathematische Werke*, **III**, 1–314, Vieweg, 1932. [English translation of the French version of the first edition: *Theory of Algebraic Integers*, Cambridge 1996.]

Dedekind,R. [77]: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers, in: *Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C.F.Gauß*, 1-55, Braunschweig 1877 = *Gesammelte mathematische Werke*, **I**, 105–158, Vieweg, 1932.

Dedekind,R. [78]: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abhandl. Kgl. Ges. Wiss. Göttingen, **23**, 1878, 1–23 = *Gesammelte mathematische Werke*, **I**, 202–232, Vieweg, 1932.

Dedekind,R. [82]: Über die Diskriminanten endlicher Körper, Abhandl. Kgl. Ges. Wiss. Göttingen, **29**, 1882, 1–56 = *Gesammelte mathematische Werke*, **I**, 351–397, Vieweg, 1930.

Dedekind,R. [92]: Über einen arithmetischen Satz von Gauss, Mitt. Deutsch. Math. Ges. Prag, 1892, 1–11 = *Gesammelte mathematische Werke*, **II**, 28–39, Vieweg, 1931.

Dedekind,R. [95]: Über die Begründung der Idealtheorie, Nachr. Ges. Wiss. Göttingen, 1895, 106–113 = *Gesammelte mathematische Werke*, **II**, 50–58, Vieweg, 1931.

Dedekind,R. [00]: Über die Anzahl von Idealklassen in reinen kubischen Zahlkörpern, J. Reine Angew. Math., **121**, 1900, 40–123 = *Gesammelte mathematische Werke*, **II**, 148–233, Vieweg, 1931.

Dedekind,R. [31]: Charakteristische Eigenschaft einklassiger Körper Ω, = *Gesammelte mathematische Werke*, **II**, 373–375, Vieweg, 1931.

Dedekind,R.,Weber,H. [82]: Theorie der algebraischen Funktionen einer Veränderlichen, J. Reine Angew. Math., **92**, 1882, 181–290 = Dedekind, *Gesammelte mathematische Werke*, **I**, 238–249, Vieweg, 1930.

Degen,C.F. [17]: *Canon Pellianus*, Havniae 1811.

Degert,G. [58]: Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **22**, 1958, 92–97.

Delange,H. [54]: Généralisation du théorème de Ikehara, Ann. Sci. École Norm. Sup., (3) **71**, 1954, 213–242.

Delaunay,B.N. [23]: Zur Bestimmung algebraischer Zahlkörper durch Kongruenzen; eine Anwendung auf die Abelsche Gleichungen, J. Reine Angew. Math., **152**, 1923, 120–123.

Delaunay,B.N.,Faddeev,D.K. [40]: *The Theory of Irrationalities of Third Degree*, Trudy Mat. Inst. Steklov., **11**, 1940, 1–340 (Russian). [English translation: Providence 1964.]

Del Corso,I. [95]: On Kronecker's use of indeterminate coefficients, Rend. Sem. Mat. Univ. Politec. Torino, **53**, 1995, 261–275.

Del Corso,I.,Dvornicich,R. [93]: A converse of Artin's density theorem: the case of cubic fields, J. Number Theory, **45**, 1993, 28–44.

Del Corso,I.,Dvornicich,R. [02]: Number fields with the same index, Acta Arith., **102**, 2002, 323–337.

Deligne,P. [73]: Les constantes des equations fonctionnelles des fonctions L, in: *Modular Functions in One Variable*, II, 501–597, Lecture Notes in Math., **349**, Springer 1973; corr.: IV, p.149, Lecture Notes in Math., **476**, Springer 1975.

Deligne,P. [76]: Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une répresentation orthogonale, Invent. math., **35**, 1976, 299–316.

Deligne,P. [79]: Valeurs de fonctions L et périodes d'intégrales, in: *Automorphic Forms, Representations and L-functions, (Corvallis 1977)*, Proc. Symposia Pure Math., **33**, 313–346.

Deligne,P.,Ribet,K.A. [80]: Values of abelian L-functions at negative integers over totally real fields, Invent. math., **35**, 1976, 299–316.

Delorme,C.,Ordaz,O.,Quiroz,D. [01]: Some remarks on Davenport's constant, Discrete Math., **237**, 2001, 119–128.

Delsarte,S. [48]: Fonctions de Möbius sur les groupes abéliens, Ann. of Math., (2) **49**, 1948, 600–609.

Dénes,P. [51]: Über Einheiten von algebraischen Zahlkörpern, Monatsh. Math., **55**, 1951, 161–163.

Dénes,P. [52a]: Über relativ-zyklische Körper vom Primzahlgrade, Publ. Math. Debrecen, **2**, 1952, 64–65.

Dénes,P. [52b]: Beweis einer Vandiverschen Vermutung bezüglich des zweiten Falles des letzten Fermatschen Satzes, Acta Sci. Math. (Szeged), **14**, 1952, 192–202.

Dénes,P. [55]: Über den zweiten Faktor der Klassenzahl und Irregularitätsgrad der irregulären Kreiskörper, Publ. Math. Debrecen, **4**, 1955/56, 163–170.

Deninger,C. [97]: Deligne periods of mixed motives, K-theory and the entropy of certain Z^n-actions., J. Amer. Math. Soc., **10**, 1997, 259–281.

Desnoux,P.J. [88]: Congruences dyadiques entre nombre de classes de corps quadratiques, Manuscripta Math., **62**, 1988, 163–179.

Deuring,M. [32]: Galoissche Theorie und Darstellungstheorie, Math. Ann., **107**, 1932, 140–144.

Deuring,M. [33]: Imaginäre quadratische Zahlkörper mit der Klassenzahl 1, Math. Z., **37**, 1933, 405–415.

Deuring,M. [35a]: Über den Tschebotareffschen Dichtigkeitssatz, Math. Ann., **110**, 1935, 414–415.

Deuring,M. [35b]: Neuer Beweis des Bauerschen Satzes, J. Reine Angew. Math., **173**, 1935, 1–4.

Deuring,M. [49]: Algebraische Begründung der komplexen Multiplikation, Abh. Math. Sem. Univ. Hamburg, **16**, 1949, 32–47.

Deuring,M. [52]: Die Struktur der elliptischen Funktionen-Körper und die Klassenkörper der imaginären quadratischen Zahlkörper, Math. Ann., **124**, 1952, 393–426.

Deuring,M. [53]: Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, Nachr. Akad. Wiss. Göttingen, 1953, 85–94; II, 1955, 13–42; III, 1956, 37–76; IV, 1957, 55–80.

Deuring,M. [68]: Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, Invent. math., **5**, 1968, 169–179.

Deuring,M. [69]: Analytische Klassenzahlformeln, in: *Number Theory and Analysis*, 55–75, Plenum 1969.

Diaz y Diaz,F. [78]: Sur le 3-rang des corps quadratiques, Publ. Math. d'Orsay, 1978, no.11, 1–93.

Diaz y Diaz,F. [83]: Valeur minima du discriminant des corps de degré 7 ayant une place réelle, C.R. Acad. Sci. Paris. **296**, 1983, 137–139.

Diaz y Diaz,F. [84]: Valeur minima de discriminant pour certains types de corps de degré 7, Ann. Inst. Fourier, **34**, 1984, no.3, 29–38.
Diaz y Diaz,F. [87]: Petits discriminants des corps de nombres totalement imaginaires de degré 8, J. Number Theory, **25**, 1987, 34–52.
Diaz y Diaz,F. [88]: Discriminant minimal et petit discriminants des corps de nombres de degré 7 avec cinq places réels, J. London Math. Soc., (2) **38**, 1988, 33–46.
Diaz y Diaz,F.,Olivier,M. [95]: Imprimitive ninth-degree number fields with small discriminants, Math. Comp., **64**, 1995, 305–321.
Dickson,L.E. [19]: *History of the Theory of Numbers*, Washington 1919–1923. [Reprints: Chelsea 1952, 1966.]
Dickson,L.E. [23a]: *Algebras and their Arithmetic*, Chicago 1923,
Dickson,L.E. *et al.* [23b]: *Algebraic Numbers*, Report of the Committee on Algebraic Numbers of the N.R.C., 1923, 1928. [Reprint: Chelsea, 1967.]
Diekert,V. [84]: Über die absolute Galoisgruppe dyadischer Zahlkörper, J. Reine Angew. Math., **350**, 1984, 152–172.
Di Franco,F.,Pace F. [85]: Arithmetical characterization of rings of algebraic integers with class number three and four, Boll. Un. Mat. Ital., (6) **4**, 1985, 63–69.
Dinghas,A. [52]: Sur un théorème de Schur concernant les racines d'une classe des équations algébriques, Norske Vid. Selsk. Forh., **25**, 1952, 17–20.
Dirichlet,P.G.L. [28]: Mémoire sur l'impossibilité de quelques équations indéterminées du cinquiéme degré, J. Reine Angew. Math., **3**, 1828, 354–375 = *Werke*, **I**, 21–46, Berlin 1889.
Dirichlet,P.G.L. [32a]: Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques, J. Reine Angew. Math., **9**, 1832, 379–389 = *Werke*, **I**, 173–188, Berlin 1889.
Dirichlet,P.G.L. [32b]: Démonstration du théorème de Fermat pour le cas de 14iémes puissances, J. Reine Angew. Math., **9**, 1832, 390–393 = *Werke*, **I**, 181–194, Berlin 1889.
Dirichlet,P.G.L. [37a]: Beweis eines Satzes ueber die arithmetische Progression, Ber. Verhandl. Kgl. Preuß. Akad. Wiss., 108–110 = *Werke*, **I**, 307–312, Berlin 1889.
Dirichlet,P.G.L. [37b]: Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abhandl. Kgl. Preuß. Akad. Wiss., 45–81 = *Werke*, **I**, 313–342, Berlin 1889. [French translation: J. math. pures appl., **4**, 1839, 393–422.]
Dirichlet,P.G.L. [38]: Sur l'usage des séries infinies dans la théorie des nombres. J. Reine Angew. Math., **18**, 1838, 259–274 = *Werke*, **I**, 357–374, Berlin 1889.
Dirichlet,P.G.L. [39]: Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. J. Reine Angew. Math., **19**, 1839, 324–369; **21**, 1840, 1–12, 134–155 = *Werke*, **I**, 411–496. G.Reimer, Berlin 1889.
Dirichlet,P.G.L. [40]: Sur la théorie des nombres, C.R. Acad. Sci. Paris, **10**, 1840, 285–288 = *Werke*, **I**, 619–623, Berlin 1889.
Dirichlet,P.G.L. [41a]: Untersuchungen über die Theorie der complexen Zahlen, J. Reine Angew. Math., **22**, 1841, 375–378 = *Werke*, **I**, 503–508, Berlin 1889.
Dirichlet,P.G.L. [41b]: Untersuchungen über die Theorie der complexen Zahlen, Abh. Kgl. Preuß. Akad. Wiss. Berlin, 1841, 141–161 = *Werke*, **I**, 509–532, Berlin 1889.
Dirichlet,P.G.L. [41c]: Einige Resultate von Untersuchungen über eine Classe homogener Functionen des dritten und höheren Grades, Verhandl. Kgl. Preuß. AW, 1841, 280–285 = *Werke*, **I**, 625–632, Berlin 1889.
Dirichlet,P.G.L. [42]: Recherches sur les formes quadratiques à coefficients et à indéterminées complexes, J. Reine Angew. Math., **24**, 1842, 291–371 = *Werke*, **I**, 535–618, Berlin 1889.

Dirichlet,P.G.L. [46]: Zur Theorie der complexen Einheiten, Verhandl. Kgl. Preuß. AW, 1846, 103–107 = *Werke*, **I**, 639–644, Berlin 1889.

Disse,A. [25]: Über die Beziehung zwischen Logarithmus und Numerus in einem p-adischen algebraischen Körper, J. Reine Angew. Math., **154**, 1925, 178–198.

Disse,A. [26]: Das Fundamentalsystem für die Logarithmen eines p-adischen algebraischen Körpers und sein Regulator, J. Reine Angew. Math., **155**, 1926, 225–250.

Dobrowolski,E. [78]: On the maximal modulus of conjugates of an algebraic integer, Bull. Acad. Pol. Sci., sér. sci. math. astr. phys., **26**, 1978, 291–292.

Dobrowolski,E. [79]: On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith., **34**, 1979, 391–401.

Dobrowolski,E. [91]: Mahler's measure of a polynomial in function of the number of its coefficients, Canad. Math. Bull., **34**, 1991, 186–195.

Dobrowolski,E.,Lawton,W.,Schinzel,A. [83]: On a problem of Lehmer, in: *Studies in Pure Mathematics, (to the Memory of Paul Turán)*, 135–144, Birkhäuser 1983.

Dodson,B. [84]: The structure of Galois groups of CM-fields, Trans. Amer. Math. Soc., **283**, 1984, 1–32.

Dodson,B. [86]: Solvable and nonsolvable CM-fields, Amer. J. Math., **108**, 1986, 75–93.

Dohmae,K. [93]: On real quadratic fields with a single class in each genus, Japan J. Math., (N.S.) **19**, 1993, 241–250.

Dohmae,K. [94]: Demijanenko matrix for imaginary abelian fields of odd conductors, Proc. Japan Acad. Sci., **70**, 1994, 292–294.

Dohmae,K. [97]: A note on Sinnott's index formula, Acta Arith., **82**, 1997, 57–67.

Draxl,P.K.J. [70]: Remarques sur le groupe de classes du composé de deux corps de nombres linéairement disjoints, Sém. Delange–Pisot–Poitou, **12**, 1970/71, exp. 24.

Dress,A. [64]: Zu einem Satz aus der Theorie der algebraischen Zahlen, J. Reine Angew. Math., **216**, 1964, 218–219.

Dress,A. [65]: Eine Bemerkung über Teilringe globaler Körper, Abh. Math. Sem. Univ. Hamburg, **28**, 1965, 133–138.

Dress,A.,Scharlau,R. [82]: Indecomposable totally positive numbers in real quadratic orders, J. Number Theory, **14**, 1982, 292–306.

Dribin,D.M. [37]: Quartic fields with the symmetric group, Ann. of Math., (2) **38**, 1937, 739–746.

Drinfeld,V.G. [74]: Elliptic modules, Mat. Sb., **94**, 1974, 594–627. (Russian)

Dubickas,A. [93]: On a conjecture of A.Schinzel and H.Zassenhaus, Acta Arith., **63**, 1993, 15–20.

Dubickas,A. [95a]: On the average difference between two conjugates of an algebraic number, Liet. Mat. Rink., **35**, 1995, 415–420.

Dubickas,A. [95b]: On algebraic numbers of small measure, Liet. Mat. Rink., **35**, 1995, 421–431.

Dubickas,A. [97a]: Algebraic conjugates outside the unit circle, in: *New Trends in Probability and Statistics, 4, (Palanga 1996)*, 11–21, Utrecht 1997.

Dubickas,A. [97b]: On the maximal conjugate of a totally real integer, Liet. Mat. Rink., **37**, 1997, 18–25.

Dubickas,A. [97c]: The maximal conjugate of a non-reciprocal algebraic integer, Liet. Mat. Rink., **37**, 1997, 168–174.

Dubickas,A. [98]: On algebraic numbers close to 1, Bull. Austral. Math. Soc., **58**, 1998, 423–434.

Dubickas,A. [99]: On intervals containing full sets of algebraic integers, Acta Arith., **91**, 1999, 379–386.

Dubickas,A. [00a]: Totally real algebraic integers in small intervals, Liet. Mat. Rink., **40**, 2000, 305–312.
Dubickas,A. [00b]: On the measure of a nonreciprocal algebraic number, Ramanujan J., **4**, 2000, 291–298.
Dubickas,A. [01]: Three problems for polynomials of small measure, Acta Arith., **98**, 2001, 279–292.
Dubickas,A. [02a]: Mahler measures close to an integer, Canad. Math. Bull., **45**, 2002, 196–203.
Dubickas,A. [02b]: The Remak height for units, Acta Math. Acad. Sci. Hungar., **97**, 2002, 1–13.
Dubickas,A.,Konyagin,S.V. [98]: On the number of polynomials of bounded measure, Acta Arith., **86**, 1998, 325–342.
Dubickas,A.,Smyth,C.J. [01a]: On the metric Mahler measure, J. Number Theory, **86**, 2001, 368–387.
Dubickas,A.,Smyth,C.J. [01b]: The Lehmer constant of an annulus, J. Théor. Nombres Bordeaux, **13**, 2001, 413–420.
Dubickas,A.,Smyth,C.J. [01c]: On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles, Proc. Edinburgh Math. Soc., (2) **44**, 2001, 1–17.
Dubois,D.W.,Steger,A. [58]: A note on division algorithmus in imaginary quadratic number fields, Canad. J. Math., **10**, 1958, 285–286.
Dubois,E.,Farhane,A. [99]: Fractions continues paramétrées et citère de Rabinowitsch, in: *Number Theory in Progress*, **I**, 111–120, de Gruyter 1999.
Dubois,E.,Levesque,C. [91]: On determining certain real quadratic fields with class number one and relating this property to continuous fractions and primality properties, Nagoya Math. J., **124**, 1991, 157–180.
Dujčev,J. [56]: On prime ideals of degree 1, Acta Math. Acad. Sci. Hungar., **7**, 1956, 71–73.
Duke,W. [89]: Some problems in the multidimensional analytic number theory, Acta Arith., **52**, 1989, 203–228.
Duke,W.,Friedlander,J.,Iwaniec,H. [95]: Class group L-functions, Duke Math. J., **79**, 1995, 1–56.
Dumitrescu,T.,Shah,T.,Zafrullah,M. [00]: Domains whose overrings satisfy ACCP, Comm. Algebra, **28**, 2000, 4403–4409.
Dummit,D.S.,Kisilevsky,H. [77]: Indices in cubic fields, in: *Number Theory and Algebra*, 29–42, Academic Press 1977.
Dürbaum,H.,Kowalsky,H.J. [53]: Arithmetische Kennzeichnung von Körpertopologien, J. Reine Angew. Math., **191**, 1981, 228–245.
Duval,D. [81]: Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type (p,p), J. Number Theory, **13**, 1981, 228–245.
Dwork,B. [56]: On the Artin root number, Amer. J. Math., **78**, 1956, 444–472.
Dzhiemuratov,U. [68]: On ideals of algebraic number fields, Izv. Akad. Nauk Uzb. SSR, **12**, 1968, no.4, 9–14. (Russian)
Eakin,P.,Heinzer,W. [73]: More noneuclidean PID's and Dedekind domains with prescribed class group, Proc. Amer. Math. Soc., **40**, 1973, 66–68.
Earnest,A.G. [87]: Exponents of the class group of imaginary abelian fields, Bull. Austral. Math. Soc., **35**, 1987, 231–246.
Earnest,A,G.,Estes,D.R. [81]: An algebraic approach to the growth of class numbers of binary quadratic lattices, Mathematika, **28**, 1981, 160–168.
Earnest,A,G., Körner,O.H. [82]: On the ideal class group of 2-power exponents, Proc. Amer. Math. Soc., **86**, 1982, 196–198.
Eda,Y. [53]: On the canonical basis of ideals, Sci. Rep. Kanazawa Univ., **2**, 1953, 15–21.

Eda,Y. [55]: A note on the general divisor problem, Sci. Rep. Kanazawa Univ., **3**, 1955, 5–9.
Eda,Y.,Nakagoshi,N. [67]: An elementary proof of the prime ideal theorem with remainder term, Sci. Rep. Kanazawa Univ., **12**, 1967, 1–12.
Edgar,H. [79]: A number field without an integral basis, Math. Mag., **52**, 1979, 248–251.
Edgar,H.,Peterson,B. [80]: Some contributions to the theory of cyclic extensions of the rationals, J. Number Theory, **12**, 1980, 77–83.
Edwards,H.M. [77]: *Fermat's Last Theorem*, Springer 1977. [Reprint: Springer 1996.]
Edwards,H.M. [80]: The genesis of ideal theory, Arch. Hist. Ex. Sci., **23**, 1980, 321–378.
Edwards,H.M. [83]: Dedekind's invention of ideals, Bull. London Math. Soc., **15**, 1983, 8–17.
Edwards,H.M. [90]: *Divisor Theory*, Birkhäuser 1990.
Edwards,H.M.,Neumann,O.,Purkert,W. [82]: Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge", Arch. Hist. Ex. Sci., **27**, 1982, 49–85.
Egami,S. [80]: The distribution of residue classes modulo $\mathfrak{A}$ in an algebraic number field, Tsukuba J.Math., **4**, 1980, 9–13.
Egami,S. [81]: Average version of Artin's conjecture in an algebraic number field, Tokyo J. Math., **4**, 1981, 203–212.
Egami,S. [84]: On finiteness of the numbers of Euclidean fields in some classes of number fields, Tokyo J. Math., **7**, 1984, 183–196.
Eichler,M. [55]: On the class number of imaginary quadratic fields and the sums of divisors of natural numbers, J. Indian Math. Soc., **19**, 1955, 153–180.
Eichler,M. [56]: Der Hilbertsche Klassenkörper eines imaginärquadratischen Zahlkörpers, Math. Z., **64**, 1956, 229–242; corr. **65**, 1956, p.214.
Eichler,M. [63]: *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser 1963.
Eie,M. [89]: On the values at negative half-integers of the Dedekind zeta function of a quadratic field, Proc. Amer. Math. Soc., **105**, 1989, 273–280.
Einsiedler,M. [99]: A generalisation of Mahler measure and its application in algebraic dynamic systems, Acta Arith., **88**, 1999, 15–29.
Eisenstein,G. [44a]: Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus den dritten Wurzeln der Einheit zusammengesetzten Zahlen, J. Reine Angew. Math., **27**, 1844, 289–310.
Eisenstein,G. [44b]: Über die Anzahl der quadratischen Formen in verschiedenen complexen Theorien, J. Reine Angew. Math., **27**, 1844, 311–316.
Elder,G.G. [95]: Galois module structure of ideals in wildly ramified cyclic extensions of degree p^2, Ann. Inst. Fourier, **45**, 1995, 625–647.
Elder,G.G.,Madan,M.L. [94]: Galois module structure of the integers in wildly ramified cyclic extensions, J. Number Theory, **47**, 1994, 138–174.
Elliott,P.D.T.A. [70a]: The distribution of power residues and certain related results, Acta Arith., **17**, 1970, 141–159.
Ellison,W.,Pesek,J.,Stall,D.S.,Lundon,W.F. [71]: A postscript to a paper of A.Baker, Bull. London Math. Soc., **3**, 1971, 75–78.
Elstrodt,J.,Grunewald,F.,Mennicke,J. [85]: On unramified A_n-extensions of quadratic number fields, Glasgow Math. J., **27**, 1985, 31–37.
Emde Boas,P.van [69]: A combinatorial problem on finite Abelian groups, II, Math.Centrum, Amsterdam, ZW 007, 1969.
Emde Boas,P.van,Kruyswijk,D. [67]: A combinatorial problem on finite Abelian groups, Math.Centrum, Amsterdam, ZW 009, 1967.

Endô,A. [73a]: On the 2-rank of the ideal class group of quadratic number fields, Mem. Fac. Sci. Kyushu Univ., **27**, 1973, 7–12.
Endô,A. [73b]: On the 2-class number of certain quadratic number fields, Mem. Fac. Sci. Kyushu Univ., **27**, 1973, 111–120.
Endô,A. [76]: On the divisibility of the class number of $Q(\sqrt[3]{n})$ by 3, Mem. Fac. Sci. Kyushu Univ., **30**, 1976, 299–311.
Endô,A. [78]: Fundamental units of certain cubic number fields with negative discriminants, Kumamoto J. Sci., **13**, 1978/79, 24–36.
Endô,A. [96]: The relative class number of certain imaginary abelian number fields, Proc. Japan Acad. Sci., **72**, 1996, 64–68.
Engstrom,H.T. [30a]: On the common index divisors of an algebraic field, Trans. Amer. Math. Soc., **32**, 1930, 223–237.
Engstrom,H.T. [30b]: The theorem of Dedekind in the ideal theory of Zolotarev, Amer. Math. Monthly, **37**, 1930, 128–129.
Ennola,V. [58]: Two elementary proofs concerning simple quadratic fields, Nordisk Mat. Tidskr., **6**, 1958, 114–117.
Ennola,V. [73a]: Conjugate algebraic integers on a circle with irrational centre, Math. Z., **134**, 1973, 337–350.
Ennola,V. [73b]: Proof of a conjecture of Morris Newman, J. Reine Angew. Math., **264**, 1973, 203–206.
Ennola,V. [75a]: Conjugate algebraic integers in an interval, Proc. Amer. Math. Soc., **53**, 1975, 259–261.
Ennola,V. [75b]: A note on a cyclotomic diophantine equation, Acta Arith., **28**, 1975, 157–159.
Ennola,V. [75c]: Solution of a cyclotomic diophantine equation, J. Reine Angew. Math., **272**, 1975, 73–91.
Ennola,V. [91]: Cubic fields with exceptional units, in: *Computational Number Theory*, 104–128, de Gruyter 1991.
Ennola,V.,Smyth,C.J. [74]: Conjugate algebraic integers on a circle, Ann. Acad. Sci. Fenn. Ser. A1, **582**, 1974, 1–31.
Ennola,V.,Smyth,C.J. [76]: Conjugate algebraic integers on a circle, Acta Arith., **29**, 1976, 147–157.
Ennola,V.,Turunen,R. [85]: On totally real cubic fields, Math. Comp., **44**, 1985, 495–519.
Epstein,P. [34]: Zur Auflösbarkeit der Gleichung $x^2 - Dy^2 = -1$, J. Reine Angew. Math., **171**, 243–252.
Erdős,P.,Chao Ko [38]: Note on the Euclidean algorithm, J. London Math. Soc., **13**, 1938, 3–8.
Erdős,P.,Stewart,C.L.,Tijdeman,R. [88]: Some Diophantine equations with many solutions, Compositio Math., **66**, 1988, 37–56.
Erdős,P.,Hall,R.R. [99]: On the angular distribution of Gaussian integers with fixed norm, Discrete Math., **200**, 1999, 87–94.
Erez,B. [91]: A survey of recent work on the square root of the inverse different, Astérisque, **198/200**, 1991, 133–152.
Ernvall,R. [75]: On the distribution mod 8 of the E-irregular primes, Ann. Acad. Sci. Fenn. Ser. A1, **1**, 1975, 195–198.
Ernvall,R. [79]: Generalized Bernoulli numbers, generalized irregular primes, and class number, Ann. Univ. Turku, **178**, 1979, 1–72.
Ernvall,R. [89]: A generalization of Herbrand's theorem, Ann. Univ. Turku, **193**, 1989, 1–15.
Ernvall,R.,Metsänkylä,T. [78]: Cyclotomic invariants and E-irregular primes, Math. Comp., **32**, 1978, 617–629; corr., **33**, 1979, p.433.

Ernvall,R.,Metsänkylä,T. [91]: Cyclotomic invariants for primes between 125 000 and 150 000, Math. Comp., **56**, 1991, 851–858.
Ernvall,R.,Metsänkylä,T. [92]: Cyclotomic invariants for primes to one million, Math. Comp., **59**, 1992, 249–250.
Esmonde,J.,Murty,M.R. [99]: *Problems in Algebraic Number Theory*, Springer 1999.
Estermann,T. [48]: On Dirichlet's L-functions, J. London Math. Soc., **23**, 1948, 275–279.
Estes,D.R. [89]: On the parity of the class number of the field of qth roots of unity, Rocky Mountain J. Math., **19**, 1989, 675–682.
Euler,L. [70]: *Vollständige Anleitung in Algebra*, St. Petersburg 1770.
Evans,R.J. [77]: Generalization of a theorem of Chowla, Houston J. Math., **3**, 1977, 343–349.
Everest,G.R. [83]: Diophantine approximation and the distribution of normal integral generators, J. London Math. Soc., (2) **28**, 1983, 227–237.
Everest,G. [98]: Measuring the height of a polynomial, Math. Intelligencer, **20**, 1998, no.3, 9–16.
Everest,G.,Ward,T. [99]: *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer 1999.
Evertse,J.H. [84]: On equations in S-units and the Thue-Mahler equation, Invent. math., **75**, 1984, 561–584.
Evertse,J.H. [99]: The number of solutions of linear equations in roots of unity, Acta Arith., **89**, 1999, 45–51.
Evertse,J.H.,Győry,K. [85]: On unit equations and decomposable form equations, J. Reine Angew. Math., **358**, 1985, 6–19.
Evertse,J.H.,Győry,K. [88a]: On the number of solutions of weighted unit equations, Compositio Math., **66**, 1988, 329–354.
Evertse,J.H.,Győry,K. [88b]: Decomposable form equations, in: *New Advances in Transcendence Theory*, 175–202, Cambridge 1988.
Evertse,J.H.,Győry,K.,Stewart,C.L.,Tijdeman,R. [88a]: On S-units equation in two unknowns, Invent. math., **92**, 1988, 461–477.
Evertse,J.H.,Győry,K.,Stewart,C.L.,Tijdeman,R. [88b]: S-unit equations and their applications, in: *New Advances in Transcendence Theory*, 110–174, Cambridge 1988.
Evertse,J.H.,Moree,P.,Stewart,C.L.,Tijdeman,R. [03]: Multivariate diophantine equations with many solutions, Acta Arith., **107**, 2003, 103–125.
Evertse,J.H.,Schlickewei,H.P. [02]: A quantitative version of the absolute subspace theorem, J. Reine Angew. Math., **548**, 2002, 21–127.
Evertse,J.H.,Schlickewei,H.P.,Schmidt,W.M. [02]: Linear equations in variables which lie in a multiplicative group, Ann. of Math., (2) **155**, 2002, 807–836.
Faddeev,D.K. [74]: On representations of algebraic numbers by matrices, Zap. Nauchn. Sem. LOMI, **96**, 1974, 89–91. (Russian)
Faddeev,D.K.,Skopin,A.I. [59]: Proof of a theorem of Kawada, Dokl. Akad. Nauk SSSR, **127**, 1959, 529–530. (Russian)
Fainleib,A.S.,Saparniyazov,O. [75]: Dispersion of the sums of real characters and moments of $L(1,\chi)$, Izv. Akad. Nauk Uzbek. SSR, 1975, no.6, 24–29. (Russian)
Fanta,E. [01]: Beweis, dass jede lineare Funktion, deren Koeffizienten dem kubischen Kreisteilungskörper entnommene ganze teilerfremde Zahlen sind, unendlich viele Primzahlen dieses Körpers darstellt, Monatsh. Math. Phys., **12**, 1901, 1–44.
Favard,J. [29]: Sur les formes décomposables et les nombres algébriques, Bull. Soc. Math. France, **57**, 1929, 50–71.
Favard,J. [30]: Sur les nombres algébriques, Mathematica, **4**, 1930, 109–113.
Feit,W. [59]: On p-regular extensions of local fields, Proc. Amer. Math. Soc., **10**, 1959, 592–595.

Fekete,M. [23]: Über die Verteilung der Wurzeln bei gewisser algebraischen Gleichungen mit ganzzahligen Koeffizienten, Math. Z., **17**, 1923, 228–249.
Fekete,M.,Szegö,G. [55]: On algebraic equations with integral coefficients whose roots belong to a given point set, Math. Z., **63**, 1955, 228–249.
Feldman,N.I.,Chudakov,N.G. [72]: On a theorem of Stark, Mat. Zametki, **11**, 1972, 329–340. (Russian)
Feng K. [82a]: The rank of a group cyclotomic units in abelian fields, J. Number Theory, **14**, 1982, 315–326.
Feng K. [82b]: On the first factor of the class number of a cyclotomic field, Proc. Amer. Math. Soc., **84**, 1982, 479–482.
Feng K. [82c]: An elementary criterion on parity of class number of cyclic number field, Sci.Sinica, A, **25**, 1982, 1032–1041.
Feng K. [85]: Arithmetic characterization of algebraic number fields with given class group, Acta Math. Sinica, **1**, 1985, 47–54.
Feng K., Zhang X. [83]: On relative integral bases of quartic cyclic number fields, Kexue Tongbao, **28**, 1983, 456–457.
Ferguson, L.B.O. [70]: Algebraic kernels of plane sets, Duke Math. J., **37**,1970, 225–230.
Ferrero,B. [77]: An explicit bound for Iwasawa's λ-invariant, Acta Arith., **33**, 1977, 405–408.
Ferrero,B. [78]: Iwasawa invariants of abelian number fields, Math. Ann., **234**, 1978, 9–24.
Ferrero,B. [80]: The cyclotomic Z_2-extension of imaginary quadratic fields, Amer. J. Math., **102**, 1980, 447–459.
Ferrero,B.,Washington,L.C. [79]: The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math., (2) **109**, 1979, 377–395.
Ferton,M.J. [72]: Sur l'anneau des entiers d'une extension diédrale de degré $2p$ d'un corps local, C.R. Acad. Sci. Paris, **274**, 1972, A1529–1532.
Ferton,M.J. [73]: Sur les idéaux des entiers d'une extension cyclique de degré premier d'un corps local, C.R. Acad. Sci. Paris, **276**, 1973, A1483–1486.
Ferton,M.J. [74]: Sur l'anneau des entiers d'extensions cycliques d'un corps local, Bull. Soc. Math. France, Mém. **37**, 1974, 69–74.
Ferton,M.J. [75]: Sur l'anneau des entiers de certains extension cycliques d'un corps local, Astérisque, **24/25**, 1975, 21–28.
Fesenko,I.B. [96]: Complete discrete valuation fields, Abelian local class field theories, in: *Handbook of Algebra*, **I**, 365–393, Elsevier 1996.
Fesenko,I.B.,Vostokov,S.V. [93]: *Local Fields and their Extensions*, Amer. Math. Soc. 1993.
Fieker,C. [01]: Computing class fields via the Artin map, Math. Comp., **70**, 2001, 1293–1303.
Flammang,V. [95]: Sur la longeur des entiers algébriques totalement positifs, J. Number Theory, **54**, 1995, 60–72.
Flammang,V. [96]: Two new points in the spectrum of the absolute Mahler measure of totally positive algebraic integers, Math. Comp., **65**, 1996, 307–311.
Flammang,V. [97]: Inégalités sur la mesure de Mahler d'un polynôme, J. Théor. Nombres Bordeaux, **9**, 1997, 69–74.
Flammang,V.,Rhin,G.,Smyth,C.J. [97]: The integer transfinite diameter of intervals and totally real algebraic integers, J. Théor. Nombres Bordeaux, **9**, 1997, 137–168.
Flanders,H. [53a]: The norm function of an algebraic field extension, Pacific J. Math., **3**, 1953, 103–113; **5**, 1955, 519–528.
Flanders,H. [53b]: Generalization of a theorem of Ankeny and Rogers, Ann. of Math., (2) **57**, 1953, 392–400.

Flanders,H. [60]: The meaning of the form calculus in classical ideal theory, Trans. Amer. Math. Soc., **95**, 1960, 92–100.
Fleischer,I. [53]: Sur les corps topologiques et les valuations, C.R. Acad. Sci. Paris, **236**, 1953, 1320–1322.
Flynn,E.V.,Poonen,B.,Schaefer,E.F. [97]: Cycles of quadratic polynomials and rational points on a genus 2-curve, Duke Math. J., **90**, 1997, 435–463.
Fogels,E. [43]: Zur Arithmetik quadratischer Zahlenkörper, Wiss. Abh. Univ. Riga, Kl. Math., **1**, 1943, 23–47.
Fogels,E. [61]: On the distribution of prime ideals, Dokl. Akad. Nauk SSSR, **140**, 1961, 1029–1032. (Russian)
Fogels,E. [62a]: On the zeros of Hecke's L-functions, Acta Arith., **7**, 1962, 87–106, 131–147, 225–240.
Fogels,E. [62b]: On the distribution of prime ideals, Acta Arith., **7**, 1962, 255–269.
Fogels,E. [63]: Über die Ausnahmenullstelle der Heckeschen L-Funktionen, Acta Arith., **8**, 1963, 307–309.
Fogels,E. [65]: On the zeros of L-functions, Acta Arith., **11**, 1965, 69–96; corr. **14**, 1967/68, p.435.
Fogels,E. [66a]: On the abstract theory of primes, Acta Arith., **10**, 1964, 137–182, 333–358, **11**, 1966, 293–331.
Fogels,E. [71]: On the zeros of of a class of L-functions, Acta Arith., **18**, 1971, 153–164.
Fogels,E. [65]: A mean value theorem of Bombieri's type, Acta Arith., **21**, 1972, 137–151.
Foote,R. [90]: Nonmonomial characters and Artin's conjecture, Trans. Amer. Math. Soc., **321**, 1990, 261–272.
Foote,R.,Murty,V.K. [89]: Zeros and poles of Artin L-series, Math. Proc. Cambridge Philos. Soc., **105**, 1989, 5–11.
Foote,R.,Wales,D. [90]: Zeros of order 2 of Dedekind zeta function and Artin's conjecture, J. Algebra, **131**, 1990, 226–257.
Ford,D. [89]: Enumeration of totally complex quartic fields of small discriminant, in: *Computational Number Theory (Debrecen 1989)*, 129–138, de Gruyter 1989.
Ford,D. [96]: Minimum discriminants of primitive sextic fields, in: *Algorithmic Number Theory (Talence 1996)*, 141–143, Lecture Notes in Comput. Sci., **1122**, Springer 1996.
Ford,D.,Pohst,M. [92]: The totally real A_5 extension of degree 6 with minimum discriminant, Exposition Math., **1**, 1992, 231–235.
Ford,D.,Pohst,M. [93]: The totally real A_6 extension of degree 6 with minimum discriminant, Exposition Math., **2**, 1993, 231–232.
Ford,D.,Pohst,M.,Daberkow,M.,Haddad,N. [98]: The S_3 extensions of degree 6 with minimum discriminant, Experiment Math., **7**, 1998, 121–124.
Forman,W.,Shapiro,H.N. [54]: Abstract prime number theorem, Comm. Pure Appl. Math., **7**, 1954, 587–619.
Fossum,R.M. [73]: *The Divisor Class Group of a Krull Domain*, Springer 1973.
Foster,L.L.T. [70]: On the number fields $Q(\vartheta)$, where $\nu^{2p} + p^2(\nu + 1) = 0$, Math. Nachr., **44**, 1970, 145–149.
Fouvry,E. [99]: Sur les propriétés de divisibilité des nombres de classes de corps quadratiques, Bull. Soc. Math. France, **127**, 1999, 95–113.
Fox,G.J.,Urbanowicz,J.,Williams,K.S. [99]: Gauss' congruence from Dirichlet's class number formula and generalizations, in: *Number Theory in Progress*, **II**, 818–839, de Gruyter 1999.
Fraenkel,A. [12]: Axiomatische Begründung von Hensel's p-adischen Zahlen, J. Reine Angew. Math., **141**, 1912, 43–76.

Fraenkel,A. [16]: *Über gewisse Teilbereiche und Erweiterungen von Ringen*, Habilitationsschrift, Leipzig 1916.

Frei,G. [81a]: Fundamental systems of units in number fields $\mathbb{Q}(\sqrt{D^2+d}, \sqrt{D^2+4d})$ with $d|D$, Archiv Math., **36**, 1981, 137–144.

Frei,G. [81b]: Fundamental systems of units in bicubic parametric number fields, Archiv Math., **36**, 1981, 524–536.

Frei,G. [82]: Fundamental systems of units in biquadratic parametric number fields, J. Number Theory, **15**, 1982, 295–303.

Frei,G.,Levesque,C. [79]: Independent system of units in certain algebraic number fields, J. Reine Angew. Math., **311/312**, 1979, 116–144.

Frei,G.,Levesque,C. [80]: On an independent system of units in the field $K = Q(\sqrt[n]{D^n \pm d})$, where $d|D^n$, Abh. Math. Sem. Univ. Hamburg, **50**, 1980, 162–165.

Freiman,G.,Geroldinger,A. [00]: An addition theorem and its arithmetical application, J. Number Theory, **85**, 2000, 59–73.

Fresnel,J. [67]: Nombres de Bernoulli généralises et fomnctions L p-adiques, Ann. Inst. Fourier, **17**, 1967, no.2, 281–333.

Fresnel,J. [71]: Valeurs des fonctions zeta aux entiers negatifs, Sém. Théor. Nombres Bordeaux, 1970/71, exp.27.

Frey,G.,Geyer,W.D. [72]: Über die Fundamentalgruppe von Körpern mit Divisorentheorie, J. Reine Angew. Math., **254**, 1972, 110–122.

Friedlander,J.B. [73]: On the least k-th power non-residue in an algebraic number field, Proc. London Math. Soc., (3) **26**, 1973, 19–34.

Friedlander,J.B. [74]: Character sums in quadratic fields, Proc. London Math. Soc., (3) **28**, 1974, 99–111.

Friedlander,J.B. [76]: On the class numbers of certain quadratic extensions, Acta Arith., **28**, 1976, 391–393.

Friedlander,J.B. [80]: Estimates for prime ideals, J. Number Theory, **12**, 1980, 101–105.

Friedman,E.C. [82a]: Ideal class groups in basic $Z_{p_1} \times \cdots \times Z_{p_s}$-extensions of abelian number fields, Invent. math., **65**, 1982, 425–440.

Friedman,E. [82b]: Iwasawa theory for several primes and connection to Wieferich's criterion, in: *Developments related to Fermat's Last theorem*, 269–294, Birkhäuser 1982.

Friedman,E. [87]: The zero near 1 of an ideal class zeta function, J. London Math. Soc., (2) **35**, 1987, 1–17.

Friedman,E. [89]: Analytic formulae for the regulator of a number field, Invent. math., **98**, 1989, 599-622.

Frobenius,G. [96]: Ueber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, SBer. Kgl. Preuß. Akad. Wiss. Berlin, 1896, 689–703.

Frobenius,G. [12]: Über quadratische Formen, die viele Primzahlen darstellen, SBer. Kgl. Preuß. Akad. Wiss. Berlin, 1912, 966–980.

Fröhlich,A. [52]: On the class group of relatively abelian fields, Quart. J. Math., Oxford ser., (2) **3**, 1952, 98–106.

Fröhlich,A. [54a]: On the absolute class group of abelian fields, J. London Math. Soc., **29**, 1954, 211–217; **30**, 1955, 72–80.

Fröhlich,A. [54b]: The generalization of a theorem of L.Rédei's, Quart. J. Math., Oxford ser., (2) **5**, 1954, 130–140.

Fröhlich,A. [54c]: A remark on the class number of abelian fields, J. London Math. Soc., **29**, 1954, p.498.

Fröhlich,A. [54d]: A remark on the class number of abelian fields, J. London Math. Soc., **29**, 1954, p.498.

Fröhlich,A. [57]: On a method of determination of class number factors in number fields, Mathematika, **4**, 1957, 113–121.
Fröhlich,A. [59]: The genus field and genus group in finite number fields, Mathematika, **16**, 1959, 40–46, 142–146.
Fröhlich,A. [60a]: A prime decomposition symbol for certain non Abelian number fields, Acta Sci. Math. (Szeged), **21**, 1960, 229–246.
Fröhlich,A. [60b]: Discriminants of algebraic number fields, Math. Z., **74**, 1960, 18–28.
Fröhlich,A. [60c]: Ideals in an extension field as modules over the algebraic integers in a finite number field, Math. Z., **74**, 1960, 29–38.
Fröhlich,A. [60d]: The discriminants of relative extensions and the existence of integral bases, Mathematika, **7**, 1960, 15–22.
Fröhlich,A. [61]: Discriminants and module invariants over a Dedekind domain, Mathematika, **7**, 1960, 15–22.
Fröhlich,A. [62a]: On non-ramified extensions with prescribed Galois group, Mathematika, **9**, 1962, 133–134.
Fröhlich,A. [62b]: The module structure of Kummer extensions over Dedekind domains, J. Reine Angew. Math., **209**, 1962, 39–53.
Fröhlich,A. [62c]: On the l-classgroup of the field $P(\sqrt[l]{m})$, J. London Math. Soc., **37**, 1962, 189–192.
Fröhlich,A. [72]: Artin root numbers and normal integral bases for quaternion fields, Invent. math., **17**, 1972, 143–166.
Fröhlich,A. [74a]: Module invariants and root numbers for quaternion fields of degree $4l^\gamma$, Proc. Cambridge Philos. Soc., **76**, 1974, 393–399.
Fröhlich,A. [74b]: Galois module structure and Artin L-functions, Proc. ICM Vancouver 1974, 351–356.
Fröhlich,A. [75]: Artin root-number for quaternion characters, Symposia Math., **15**, 1975, 353–363.
Fröhlich,A. [76a]: A normal integral basis theorem, J. Algebra, **39**, 1976, 131–137.
Fröhlich,A. [76b]: Arithmetic and Galois module structure for tame extensions, J. Reine Angew. Math., **286/287**, 1976, 380–440.
Fröhlich,A. [77a]: Galois module structure, in: *Algebraic Number Fields*, 133–191, Academic Press 1977.
Fröhlich,A. [77b]: Stickelberger without Gauss sums, in: *Algebraic Number Fields*, 589–607, Academic Press 1977.
Fröhlich,A. [77c]: Non-abelian Jacobi sums, in: *Number Theory and Algebra*, 71–75, Academic Press 1977.
Fröhlich,A. [78]: Some problems of Galois module structure for wild extensions, Proc. London Math. Soc., (3) **37**, 1978, 193–212.
Fröhlich,A. [83a]: *Galois Module Structure of Algebraic Integers*, Springer 1983.
Fröhlich,A. [83b]: *Central Extensions, Galois Groups and Ideal Class Groups of Number Fields*, Contemp. Math., **24**, 1983.
Fröhlich,A. [83c]: *Gaussche Summen*, I,II, Univ. Köln 1983.
Fröhlich,A. [89]: L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure), J. Reine Angew. Math., **397**, 1989, 42–99.
Fröhlich,A.,Keating,M.,Wilson,S. [74]: The classgroup of dihedral 2-groups, Mathematika, **21**, 1974, 64–71.
Fröhlich,A.,Queyrut,J. [73]: On the functional equation of the Artin L-function for characters of real representations, Invent. math., **20**, 1973, 125–138.
Fröhlich,A.,Serre,J.P.,Tate,J. [62]: A different with an odd class, J. Reine Angew. Math., **209**, 1962, 6–7.

Fröhlich,A.,Taylor,M. [80]: The arithmetic theory of local Gauss sums for tame characters, Philos. Trans. Roy. Soc. London, A, **298**, 1980/81, 141–181.

Fröhlich,A.,Taylor,M. [93]: *Algebraic Number Theory*, Cambridge University Press 1993.

Fryska,T. [79]: Über die obere Grenze der rellen Teile der Nullstellen der Dedekindschen Zetafunktionen, Funct. Approx. Comment. Math., **7**, 1979, 91–99.

Fryska,T. [91]: Von der Reihe $\sum_\rho x^\rho/\rho$, Lit. Mat. Sb., **31**, 1991, 187–204.

Fuchs,L. [63]: Ueber die Perioden, welche aus den Wurzeln der Gleichung $w^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, J. Reine Angew. Math., **61**, 1863, 374–386.

Fuchs,L. [66]: Ueber die aus Einheitswurzeln gebildeten complexen Zahlen von periodischen Verhalten, insbesondere die Bestimmung der Klassenzahl derselben, J. Reine Angew. Math., **65**, 1866, 74–111.

Fuchs,L. [48]: A theorem on the relative norm of an ideal, Comment. Math. Helv., **21**, 1948, 29–43.

Fuchs,P. [97]: Maillet's determinant and a certain basis of the Stickelberger ideal, Tatra Mt. Math. Publ., **11**, 1997, 121–128.

Fueter,R. [05]: Die Theorie der Zahlstrahlen, J. Reine Angew. Math., **130**, 1905, 197–237; II, **132**, 1907, 255–269.

Fueter,R. [07]: Die Klassenzahl der Körper der komplexen Multiplikation, Nachr. Ges. Wiss. Göttingen, 1907, 288–298.

Fueter,R. [10]: Die verallgemeinerte Kroneckersche Grenzformel und ihre Anwendung auf die Berechnung der Klassenzahl, Rend. Circ. Mat. Palermo, **29**, 1910, 380–395.

Fueter,R. [11]: *Die Klassenkörper der komplexen Multiplikation und ihr Einfluss auf die Entwicklung der Zahlentheorie*, Jahresber. Deutsch. Math.-Verein., **20**, 1911, 1–47.

Fueter,R. [14]: Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern, Math. Ann., **75**, 1914, 177–255.

Fueter,R. [17]: Die Klassenzahl zyklischer Körper vom Primzahlgrad, deren Diskriminante nur eine Primzahl enthält, J. Reine Angew. Math., **147**, 1917, 174–183.

Fueter,R. [24]: *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Teubner 1924-1927.

Fujii,A. [77]: A remark on the zeros of some L-functions, Tôhoku Math. J., (2) **29**, 1977, 417–426.

Fujisaki,G. [74]: Note on a paper of E.Artin, Sci. Papers College Gen. Ed. Univ. Tokyo, **23**, 1973, 1–3.

Fujisaki,G. [90]: A remark on quaternionic extensions of the rational p-adic field, Proc. Japan Acad. Sci., **66**, 1990, 257–259.

Fujita,H. [93]: The minimum discriminant of totally real algebraic number fields of degree 9 with cubic subfields, Math. Comp., **60**, 1993, 801–910; II, Saitama Math. J., **9**, 1991, 9–18.

Fujiwara,M. [72]: Hasse principle in algebraic equations, Acta Arith., **22**, 1972, 267–276.

Fujiwara,M.,Sudo,M. [76]: Some forms of odd degree for which the Hasse principle fails, Pacific J. Math., **67**, 1976, 161–169.

Fukuda,T. [97]: On the vanishing of Iwasawa invariants of certain cyclic extension of Q with prime degree, Proc. Japan Acad. Sci., **73**, 1997, 108–110.

Fukuda,T.,Komatsu,K. [00]: Ichimura-Sumuda criterion for Iwasawa λ-invariants, Proc. Japan Acad. Sci., **76**, 2000, 111–115.

Funakura,T. [84]: On integral bases for pure quartic fields, Math. J. Okayama Univ., **26**, 1984, 27–41.

Funakura,T. [92]: A generalization of the Chowla-Mordell theorem on Gaussian sums, Bull. London Math. Soc., **24**, 1992, 424–430.
Fung,G.,Granville,A.,Williams,H.C. [92]: Computation of the first factor of the class number of cyclotomic fields, J. Number Theory, **42**, 1992, 297–312.
Fung,G.,Williams,H.C. [90]: On the computation of a table of complex cubic fields with discriminant $D > -10^6$, Math. Comp., **55**, 1990, 313–325; errata: **63**, 1994, p.433.
Furtwängler,Ph. [04]: Über die Reziprozitätsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet, Math. Ann., **58**, 1904, 1–50.
Furtwängler,Ph. [07]: Allgemeiner Existenzbeweis für den Klassenkörper eines beliebiges algebraischen Zahlkörpers, Math. Ann., **63**, 1907, 1–37.
Furtwängler,Ph. [08]: Über die Klassenzahl Abelscher Zahlkörper, J. Reine Angew. Math., **134**, 1908, 91–94.
Furtwängler,Ph. [09]: Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten, Math. Ann., **67**, 1909, 1–31; **72**, 1912, 346–386; **74**, 1913, 413–429.
Furtwängler,Ph. [11]: Über die Klassenzahl der Kreisteilungskörper, J. Reine Angew. Math., **140**, 1911, 29–32.
Furtwängler,Ph. [16]: Über das Verhalten der Ideale des Grundkörpers in Klassenkörper, Monatsh. Math. Phys., **27**, 1916, 1–15.
Furtwängler,Ph. [19]: Über die Führer der Zahlringe, Ber. Akad. Wiss. Wien, **128**, 1919, 239–245.
Furtwängler,Ph. [30]: Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **7**, 1930, 14–36.
Furuta,Y. [59]: On meta-abelian fields of a certain type, Nagoya Math. J., **14**, 1959, 193–199.
Furuta,Y. [61]; A property of meta-abelian extensions, Nagoya Math. J., **19**, 1961, 169–187.
Furuta,Y. [66]: The notion of restricted idèles with applications to some extension fields, Nagoya Math. J., **27**, 1966, 121–132; II, J. Math. Soc. Japan, **18**, 1966, 247–252.
Furuta,Y. [71]: Über die zentrale Klassenzahl eines relativ-galoisschen Zahlkörpers, J. Number Theory, **3**, 1971, 318–322.
Furuta,Y. [72]: On class field towers and the rank of ideal class groups, Nagoya Math. J., **48**, 1972, 147–157.
Furuta,Y. [76]: On nilpotent factors of congruent ideal class groups, Nagoya Math. J., **48**, 1972, 147–157.
Furuta,Y. [77]: Note on class number factors and prime decomposition, Nagoya Math. J., **66**, 1977, 167–182.
Furuya,H. [71]: On divisibility by 2 of the relative class numbers of imaginary number fields, Tôhoku Math. J., (2) **23**, 1971, 207–218.
Furuya,H. [77]: Principal ideal theorems in the genus field for absolutely Abelian extensions, J. Number Theory, **9**, 1977, 4–15.
Furuya,H. [82]: Ambiguous numbers over $P(\zeta_3)$ of absolutely Abelian extensions of degree 6, Tokyo J. Math., **5**, 1982, 457–462.
Gaál,I. [95]: Computing elements of given index in totally complex cyclic sextic fields, J. Symbolic Comp., **20**, 1995, 61–69.
Gaál,I. [98]: Power integral bases in composita of number fields, Canad. Math. Bull., **41**, 1998, 158–165.
Gaál,I. [02]: *Diophantine Equations and Power Integral Bases*, Birkhäuser 2002.
Gaál,I., Győry,K. [99]: Index form equations in quintic fields, Acta Arith., **89**, 1999, 379–396.

Gaál,I.,Nyul,G. [01]: Computing all monogeneous mixed dihedral quartic extensions of a quadratic field, J. Théor. Nombres Bordeaux, **13**, 2001, 137–142.
Gaál,I.,Olajos,P.,Pohst,M. [01]: Power integral bases in orders of composite fields, Experiment Math., **11**, 2001, 87–90.
Gaál,I.,Pethö,A.,Pohst,M. [91]: On the indices of biquadratic number fields having Galois group V_4, Archiv Math., **57**, 1991, 57–361.
Gaál,I.,Pohst,M. [96]: On the resolution of index form equations in sextic fields with an imaginary quadratic subfield, J. Symbolic Comp., **22**, 1996, 425–434.
Galkin,V.M. [72]: The first factor of the class number of ideals of a cyclotomic field, Uspekhi Mat. Nauk, **27**, 1972, no.6, 233–234. (Russian)
Gao,W. [97]: On a combinatorial problem connected with factorizations, Colloq. Math., **72**, 1997, 251–268.
Gao,W. [00]: On Davenport's constant of finite abelian groups with rank three, Discrete Math., **222**, 2000, 11–124.
Gao,W.,Geroldinger,A. [98]: Half-factorial domains and half-factorial subsets of abelian groups, Houston J. Math., **24**, 1998, 593–611.
Gao,W.,Geroldinger,A. [00]: Systems of sets of lengths, II, Abh. Math. Sem. Univ. Hamburg, **70**, 2000, 31–49.
Garbanati,D.A. [75]: Extensions of the Hasse norm theorem, Bull. Amer. Math. Soc., **81**, 1975, 583–586; II, Lin. Multilin. Algebra, **3**, 1975/76, 143–145.
Garbanati,D.A. [76]: Units of norm -1 and signatures of units, J. Reine Angew. Math., **283/284**, 1976, 164–175.
Garbanati,D.A. [77]: The Hasse norm theorem for l-extensions of the rationals, in: *Number Theory and Algebra*, 77–90, Academic Press 1977.
Garbanati,D.A. [78a]: Invariants of the ideal class group and the Hasse norm theorem, J. Reine Angew. Math., **297**, 1978, 159–171.
Garbanati,D.A. [78b]: The Hasse norm theorem for noncyclic extensions of the rationals, Proc. London Math. Soc., (3) **37**, 1978, 143–164.
Garbanati,F.A. [80]: An algorithm for finding an algebraic number whose norm is a given rational number, J. Reine Angew. Math., **316**, 1980, 1–13.
Gassmann,F. [26]: Bemerkungen zu der bevorstehender Arbeit von Hurwitz, Math. Z., **25**, 1926, 665–675.
Gathen,J.von zur,Panario,D. [01]: Factoring polynomials over finite fields: a survey, J. Symbolic Comp., **31**, 2001, 3–17.
Gauss,C.F. [01]: *Disquisitiones Arithmeticae*, Göttingen 1801. [English translation: Yale Univ. Press 1966; German translation: Chelsea 1965; Russian translation: Moskva 1959.]
Gauss,C.F. [11]: Summatio quarumdam serierum singularium, Comm. Soc. Reg. Sci. Gotting., **1**, 1811 = *Werke*, **II**, 9–45, Göttingen 1863.
Gauss,C.F. [28]: Letter to Dirichlet of May, 30th, 1828 in: Dirichlet, *Werke*, **II**, 378–380, Göttingen 1863.
Gauss,C.F. [32]: Theoria residuorum biquadraticorum, Comm. Soc. Reg. sc. Gotting., **7**, 1832 = *Werke*, **II**, 93–198, Göttingen 1863.
Gauthier,F. [78]: Ensembles de Kronecker et representations des nombres premiers par une forme quadratique binaire, Bull. Sci. Math., (2) **102**, 1978, 129–143.
Gelbart,S. [77]: Automorphic forms and Artin's conjecture, in: *Modular Forms in One Variable*, **VI**, 241–276, Lecture Notes in Math., **627**, Springer 1977; II, Mitt. Math. Ges. Hamburg, **12**, 1991, 907–947.
Gelbart,S. [84]: An elementary introduction to the Langlands program, Bull. Amer. Math. Soc., (N.S.) **10**, 1984, 177–219.
Gelfond,A.O. [53]: On an elementary approach to some problems from the field of distribution of prime numbers, Vestnik MGU, **8**, 1953, no.2, 21–26. (Russian)

Gelfond,A.O. [60]: Some functional equations implied by equations of Riemann type, Izv. Akad. Nauk SSSR, Ser. Mat., **24**, 1960, 469–474. (Russian)
Gérardin,P.,Labesse,J.P. [79]: The solution of a base change problem for $GL(2)$, Proc. Symposia Pure Math., **33**, 1979, II, 115–133.
Gerlovin,É.L. [69]: The completion of the multiplicative group of a cyclic p-extension of a local field, Vestnik LGU, **22**, 1969, no.7, 14–22. (Russian)
Geroldinger,A. [88]: Über nicht–eindeutige Zerlegungen in irreduzible Elemente, Math. Z., **197**, 1988, 505–529.
Geroldinger,A. [89]: Factorizations of algebraic integers, in: *Number Theory (Ulm 1987)*, 63–74, Lecture Notes in Math., **1380**, Springer 1989.
Geroldinger,A. [90a]: Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern, Math. Z., **205**, 1990, 159–162.
Geroldinger,A. [90b]: Systeme von Längenmengen, Abh. Math. Sem. Univ. Hamburg, **60**, 1990, 115–130.
Geroldinger,A. [90c]: On non-unique factorizations into irreducible integers, II, in: *Number Theory, (Budapest 1987)*, II, 723–757, North Holland 1990.
Geroldinger,A. [90d]: Arithmetical characterizations of divisor class group, Archiv Math., **54**, 1990, 455–464; II, Acta Math. Univ. Comenian., (N.S.) **61**, 1992, 193–208.
Geroldinger,A. [91]: Factorization of natural numbers in algebraic number fields, Acta Arith., **57**, 1991, 365–373.
Geroldinger,A. [94]: T-block monoids and their arithmetic applications to certain integral domains, Comm. Algebra, **22**, 1994, 1603–1615.
Geroldinger,A. [97a]: Chains of factorizations in weakly Krull domains, Colloq. Math., **72**, 1997, 53–81.
Geroldinger,A. [97b]: Chains of factorizations in orders of global fields, Colloq. Math., **72**, 1997, 83–102.
Geroldinger,A. [97c]: Chains of factorizations and sets of lengths, J. Algebra, **188**, 1997, 331–362.
Geroldinger,A. [98]: A structure theorem for sets of lengths, Colloq. Math., **78**, 1998, 225–259.
Geroldinger,A.,Gao,W. [90]: Factorization problems in semigroups, Semigroup Forum, **40**, 1990, 23–38.
Geroldinger,A.,Halter-Koch,F., [92a]: Nonunique factorization in block semigroups and arithmetical applications, Math. Slovaca, **42**, 1992, 641–661.
Geroldinger,A.,Halter-Koch,F., [92b]: On the asymptotic behaviour of lengths of factorizations, J. Pure Appl. Algebra, **77**, 1992, 239–252.
Geroldinger,A.,Halter-Koch,F.,Kaczorowski,J. [95]: Non–unique factorizations in orders of global fields, J. Reine Angew. Math., **459**, 1995, 89–118.
Geroldinger,A.,Kaczorowski,J. [92]: Analytic and arithmetic theory of semigroups with divisor theory, J. Théor. Nombres Bordeaux, **4**, 1992, 199–238.
Geroldinger,A.,Lettl,G. [90]: Factorization problems in semigroups, Semigroup Forum, **40**, 1990, 23–38.
Geroldinger,A.,Schneider,R. [92]: On Davenport's constant, J.Comb. Theory, A **61**, 1992, 147–152.
Gerst,I. [70]: On the theory of nth power residues and a conjecture of Kronecker, Acta Arith., **17**, 1970, 121–139.
Gerst,I.,Brillhart,J. [71]: On the prime divisors of polynomials, Amer. Math. Monthly, **71**, 1971, 250–266.
Gerth,F.III. [73]: Ranks of Sylow 3-subgroups of ideal class group of certain cubic fields, Bull. Amer. Math. Soc., **79**, 1973, 521–525.
Gerth,F.III. [75a]: On 3-class groups of pure cubic fields, J. Reine Angew. Math., **278/279**, 1975, 52–62.

Gerth,F.III. [75b]: Number fields with prescribed l-class group, Proc. Amer. Math. Soc., **49**, 1975, 284–288.
Gerth,F.III. [75c]: A note on the l-class groups of number fields, Math. Comp., **29**, 1975, 1135–1137.
Gerth,F.III. [76a]: On l-class groups of certain number fields, Mathematika, **23**, 1976, 116–123.
Gerth,F.III. [76b]: Cubic fields whose class numbers are not divisible by 3, Illinois J. Math., **20**, 1976, 84–98.
Gerth,F.III. [76c]: Ranks of 3-class groups of non-Galois cubic fields, Acta Arith., **30**, 1976, 307–322.
Gerth,F.III. [76d]: On 3-class groups of cyclic cubic extensions of certain number fields, J. Number Theory, **8**, 1976, 84–98.
Gerth,F.III. [77a]: The Hasse norm principle in metacyclic extensions of number fields, J. London Math. Soc., (2) **16**, 1977, 203–208.
Gerth,F.III. [77b]: The Hasse norm principle for abelian extensions of number fields, Bull. Amer. Math. Soc., **83**, 1977, 264–266.
Gerth,F.III. [78]: The Hasse norm principle in cyclotomic fields, J. Reine Angew. Math., **303/304**, 1978, 249–252.
Gerth,F.III. [79b]: Upper bound for an Iwasawa invariant, Compositio Math., **39**, 1979, 3–10.
Gerth,F.III. [79b]: The Iwasawa invariant μ for quadratic fields, Pacific J. Math., **80**, 1979, 131–136.
Gerth,F.III. [80]: The ideal class group of two cyclotomic fields, Proc. Amer. Math. Soc., **78**, 1980, 321–323.
Gerth,F.III. [82]: Counting certain number fields with prescribed l-class numbers, J. Reine Angew. Math., **337**, 1982, 195–207.
Gerth,F.III. [83a]: Asymptotic results for class number divisibility in cyclotomic fields, Canad. Math. Bull., **26**, 1983, 229–234.
Gerth,F.III. [83b]: An application of matrices over finite fields to algebraic number theory, Math. Comp., **41**, 1983, 229–234.
Gerth,F.III. [83c]: Asymptotic behavior of number fields with prescribed l-class numbers, J. Number Theory, **17**, 1983, 191–203.
Gerth,F.III. [83d]: Sufficiency of genus theory for certain number fields, Exposition Math., **1**, 1983, 357–359.
Gerth,F.III. [84]: The 4-class ranks of quadratic fields, Invent. math., **77**, 1984, 489–515.
Gerth,F.III. [86]: Densities for 3-class rank of pure cubic fields, Acta Arith., **46**, 1986, 227–242; corr. **50**, 1988, p.405.
Gerth,F.III. [87a]: Densities for 3-class rank in certain cubic extensions, J. Reine Angew. Math., **381**, 1987, 161–180.
Gerth,F.III. [87b]: Densities for ranks of certain parts of p-class groups, Proc. London Math. Soc., (3) **99**, 1987, 1–8.
Gerth,F.III. [89a]: The 4-class ranks of quadratic extensions of certain imaginary quadratic fields, Illinois J. Math., **33**, 1989, 132–142.
Gerth,F.III. [89b]: The 4-class ranks of quadratic extensions of certain real quadratic fields, J. Number Theory, **33**, 1989, 18–31.
Gerth,F.III. [89c]: On p-class groups of cyclic extensions of prime degree p of quadratic fields, Mathematika, **36**, 1989, 89–102.
Gerth,F.III. [90]: On p-class groups of cyclic extensions of prime degree p of certain cyclotomic fields, Manuscripta Math., **70**, 1990, 39–50.
Gerth,F.III. [91]: On p-class groups of cyclic extensions of prime degree p of number fields, Acta Arith., **60**, 1991, 85–92.

Gerth,F.III. [93]: Some results on the capitulation problem for quadratic fields, Exposition Math., **11**, 1993, 185–192.
Gerth,F.III. [98]: On 2-class field towers for quadratic number fields with 2-class group of type $(2,2)$, Glasgow Math. J., **40**, 1998, 63–69.
Gerth,F.III. [01]: Comparison of 4-class ranks of certain quadratic fields, Proc. Amer. Math. Soc., **129**, 2001, 2547–2552.
Gerth,F.III. [03]: Quadratic fields with infinite Hilbert 2-class field towers, Acta Arith., **106**, 2003, 151–158.
Gethner,E.,Stark,H.M. [97]: Periodic Gaussian moats, Experiment Math., **6**, 1997, 289–292.
Gethner,E.,Wagon,S.,Wick,B. [98]: A stroll through the Gaussian primes, Amer. Math. Monthly, **105**, 1998, 327–337.
Geyer,W.D. [78]: The automorphism group of the field of all algebraic numbers, in: *Proceedings of the 5th School of Algebra*, 167–199, Rio de Janeiro 1978.
Ghate,E. [00]: The Kronecker-Weber theorem, in: *Cyclotomic Fields and Related Topics (Pune 1999)*, 135–146, Pune 2000.
Gilbarg,D. [42]: The structure of the group of $\mathfrak{p}$-adic 1-units, Duke Math. J., **9**, 1942, 262–271.
Gillard,R. [76]: Remarques sur certains extensions prodiédrales de corps de nombres, C.R. Acad. Sci. Paris, **282**, 1976, 13–15.
Gillard,R. [77]: Sur le groupe des classes des extensions abéliennes réelles, Sém. Delange–Pisot–Poitou, **18**, 1976/77, exp.10.
Gillard,R. [79a]: Unités elliptiques et unités cyclotomiques, Math. Ann., **243**, 1979, 181–189.
Gillard,R. [79b]: Remarques sur les unités cyclotomiques et unités elliptiques, J. Number Theory, **11**, 1979, 21–48.
Gillard,R. [79c]: Unités cyclotomiques, unités semilocales et Z_l-extensions, Ann. Inst. Fourier, **29**, 1977, no. 1, 49–79; II, no.4, 1–15.
Gillard,R. [79d]: Formulation de la conjecture de Leopoldt et étude d'une condition suffisante, Abh. Math. Sem. Univ. Hamburg, **48**, 1979, 125–138.
Gillard,R. [80a]: Unités elliptiques et unités de Minkowski, J. Math. Soc. Japan, **32**, 1980, 697–701.
Gillard,R. [80b]: Unités elliptiques et fonctions L p-adiques, Compositio Math., **42**, 1980/81, 57–88.
Gillard,R.,Robert,G. [79]: Groupes d'unités elliptiques, Bull. Soc. Math. France, **107**, 1979, 305–317.
Gilmer,R.W.Jr. [63b]: Finite rings having a cyclic multiplicative group of units, Amer. J. Math., **85**, 1963, 447–452.
Gilmer,R.W.Jr. [68]: *Multiplicative Ideal Theory*, Kingston 1968; 2nd ed., New York 1972; 3rd ed. Kingston 1992.
Gilmer,R.W.Jr. [69]: A note on generating sets for invertible ideals, Proc. Amer. Math. Soc., **22**, 1969, 426–427.
Gilmer,R.W.Jr. [72]: On commutative rings of finite rank, Duke Math. J., **39**, 1972, 381–383.
Gilmer,R.W.Jr. [73]: The n-generator property for commutative rings, Proc. Amer. Math. Soc., **38**, 1973, 477–482.
Giorgiutti,J. [60]: Modules projectifs sur les algébres de groupes finis, C.R. Acad. Sci. Paris, **250**, 1960, 1419–1420.
Girstmair,K. [79]: Elementare Berechnung von kubischen Diskriminanten, Archiv Math., **32**, 1979, 341–343.
Girstmair,K. [91]: A recursion formula for the relative class number of the p^nth cyclotomic field, Abh. Math. Sem. Univ. Hamburg, **61**, 1991, 131–138.

Girstmair,K. [92a]: On the branch order of the ring of integers of an abelian number field, Acta Arith., **62**, 1992, 297–301.
Girstmair,K. [92b]: On the trace of the ring of integers of an abelian number field, Acta Arith., **62**, 1992, 383–389.
Girstmair,K. [93]: The relative class number of imaginary cyclic fields of degrees 4, 6, 8 and 10, Math. Comp., **61**, 1993, 881–887.
Girstmair,K. [96]: A remark on normal bases, J. Number Theory, **58**, 1966, 64–65.
Glaisher,J.W.L. [03]: On the expression for the number of classes of a negative discriminant, Quart. J. Math., Oxford ser., **34**, 1903, 178–204.
Glesser,P. [89]: Inégalités sur la mesure des polynômes, Rend. Sem. Fac. Sci, Univ. Cagliari, **59**, 1989, 1–14; J. Théor. Nombres Bordeaux, **14**, 2002, 241–248.
Godin,M.,Sodaïgui,B. [02]: Classes de Steinitz d'extensions à groupe de Galois A_4,
Godin,M.,Sodaïgui,B. [03]: Module structure of rings of integers in octahedral extensions, Acta Arith., **109**, 2003, 321–327.
Godwin,H.J. [56]: Real quartic fields with small discriminants, J. London Math. Soc., **31**, 1956, 478–485.
Godwin,H.J. [57a]: On totally complex quartic fields with small discriminant, Proc. Cambridge Philos. Soc., **53**, 1957, 1–4.
Godwin,H.J. [57b]: On quartic fields with signature one with small discriminants, Quart. J. Math., Oxford ser., (2) **8**, 1957, 214–222.
Godwin,H.J. [60]: The determination of units in totally real cubic fields, Proc. Cambridge Philos. Soc., **56**, 1960, 318–321.
Godwin,H.J. [84]: A note on Cusick's theorem on units in totally real cubic fields, Math. Proc. Cambridge Philos. Soc., **95**, 1984, 1–2.
Godwin,H.J. [86]: A parametrized set of cyclic cubic fields with even class number, J. Number Theory, **22**, 1986, 246–248.
Gogia,S.K.,Luthar,I.S. [78]: Quadratic unramified extensions of $Q(\sqrt{d})$, J. Reine Angew. Math., **298**, 1978, 108—111.
Gogia,S.K.,Luthar,I.S. [79]: Real characters of the ideal class-group and the narrow ideal class-group of $Q(\sqrt{d})$, Colloq. Math., **41**, 1979/80, 153–159.
Gold,R. [74a]: Examples of Iwasawa invariants, Acta Arith., **26**, 1974, 21–32, 233–240.
Gold,R. [75]: Genera in abelian extensions, Proc. Amer. Math. Soc., **47**, 1975, 25–28.
Gold,R. [76a]: Genera in normal extensions, Pacific J. Math., **63**, 1976, 397–400.
Gold,R. [76b]: Z_3-invariants and imaginary quadratic fields, J. Number Theory, **8**, 1976, 420–423.
Gold,R. [77]: The principal genus and Hasse's norm theorem, Indiana Univ. Math. J., **26**, 1977, 183–189.
Gold,R.,Madan,M.L. [78]: Some applications of Abhyankar's lemma, Math. Nachr., **82**, 1978, 115–119.
Goldfeld,D. [73]: A large sieve for a class of nonabelian L-functions, Israel J. Math., **14**, 1973, 39–49.
Goldfeld,D. [74]: A simple proof of Siegel's theorem, Proc. Nat. Acad. Sci. U.S.A., **71**, 1974, p.1055.
Goldfeld,D. [75]: An asymptotic formula relating the Siegel zero and the class number of quadratic fields, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., (4) **2**, 1976, 611–615.
Goldfeld,D. [76]: The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., (4) **3**, 1976, 623–663.
Goldfeld,D. [77]: The conjectures of Birch and Swinnerton-Dyer and the class number of quadratic fields, Astérisque, **41/42**, 219–227.

Goldfeld,D.,Schinzel,A. [75]: On Siegel's zero, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., (4) **2**, 1975, 571–583.
Goldstein,L.J. [68]: Analogues of Artin's conjecture, Bull. Amer. Math. Soc., **74**, 1968, 517–519.
Goldstein,L.J. [70a]: A generalization of the Siegel-Walfisz theorem, Trans. Amer. Math. Soc., **149**, 1970, 417–429.
Goldstein,L.J. [70b]: Analogues of Artin's conjecture, Trans. Amer. Math. Soc., **149**, 1970, 431–442.
Goldstein,L.J. [71a]: Density questions in algebraic number theory, Amer. Math. Monthly, **78**, 1971, 342–351.
Goldstein,L.J. [71b]: A generalization of Stark's theorem, J. Number Theory, **3**, 1971, 323–346.
Goldstein,L.J. [71c]: *Analytic Number Theory*, Prentice Hall 1971.
Goldstein,L.J. [73a]: Some remarks on arithmetic density questions, Proc. Symposia Pure Math., **24**, 1973, 103–110.
Goldstein,L.J. [73b]: On a conjecture of Hecke concerning elementary class number formulas, Manuscripta Math., **9**, 1973, 245–305.
Goldstein,L.J. [73c]: On the class numbers of cyclotomic fields, J. Number Theory, **5**, 1973, 58–63
Goldstein,L.J. [74]: On a formula of Hecke, Israel J. Math., **17**, 1974, 283–301.
Goldstein,L.J.,Razar,M. [76]: A generalization of Dirichlet's class number formula, Duke Math. J., **43**, 1976, 349–358.
Goldstein,L.J.,Torre, P. de la [75]: On a function analogous to $\log \eta(\tau)$, Nagoya Math. J., **59**, 1975, 169–198.
Golod,E.S., Shafarevich,I.R. [64]: On the class-field tower, Izv. Akad. Nauk SSSR, Ser. Mat., **29**, 1964, 261–272. (Russian)
Gómez Ayala,E.J. [94]: Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Théor. Nombres Bordeaux, **6**, 1994, 95–116.
Gómez Ayala,E.J. [95]: Structure galoisienne et corps de classes de rayon de conducteur 2, Acta Arith., **72**, 1995, 375–383.
Gómez Ayala,E.J. [96]: Normal bases for quadratic extensions inside cyclotomic fields, Archiv Math., **66**, 1996, 123–125.
Gómez Ayala,E.J.,Schertz,R. [93]: Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern, J. Number Theory, **44**, 1993, 41–46.
Gonzalez,N. [99]: Elasticity and ramification, Comm. Algebra, **27**, 1999, 1729–1736.
Gorenstein,D. [82]: *Finite Simple Groups*, Plenum Press 1982.
Goss,D. [80]: The algebraist's upper plane, Bull. Amer. Math. Soc., (N.S.) **2**, 1980, 391–415.
Gouvêa,F.Q. [93]: *p-adic Numbers*, Springer 1993.
Grams,A. [74]: The distribution of prime ideals of a Dedekind domain, Bull. Austral. Math. Soc., **11**, 1974, 429–441.
Grandcolas,M. [98a]: Weighted diameters of complete sets of conjugate algebraic integers, Bull. Austral. Math. Soc., **57**, 1998, 25–36.
Grandcolas,M. [98b]: Diameters of complete sets of conjugate algebraic integers of small degree, Math. Comp., **67**, 1998, 821–831.
Grandet-Hugot,M. [66]: Étude de certaines suites $\{\lambda\alpha^n\}$ dans les adéles, Ann. Sci. École Norm. Sup., (3) **83**, 1966, 171–185.
Grandet-Hugot,M. [75]: Quelques résultats concernant l'équirépartition dans l'anneau des adéles d'un corps de nombres algébriques, Bull. Soc. Math. France, (2) **99**, 1975, 91–111; corr.: 243–247.
Grandjot,K. [24]: Über die Irreduzibilität der Kreisteilungsgleichung, Math. Z., **19**, 1924, 128–129.

Grant,D. [96]: Sequences of fields with many solutions to the unit equation, Rocky Mountain J. Math., **26**, 1996, 1017–1029.
Granville,A.J. [90]: On the size of the first factor of the class number of a cyclotomic field, Invent. math., **100**, 1990, 321–338.
Granville,A.J.,Mollin,R.A. [00]: Rabinowitsch revisited, Acta Arith., **96**, 2000, 139–153.
Granville,A.J.,Mollin,R.A.,Williams,H.C. [00]: An upper bound for the least inert prime in a real quadratic field, Canad. J. Math., **52**, 2000, 369–380.
Granville,A.J.,Stark,H.M. [00]: *ABC* implies no "Siegel zero" for L-functions of characters with negative discriminant, Invent. math., **139**, 2000, 509–523.
Gras,G. [72a]: Remarques sur la conjecture de Leopoldt, C.R. Acad. Sci. Paris, **274**, 377–380.
Gras,G. [72b]: Sur le groupe des classes des extensions cycliques de degré premier l, C.R. Acad. Sci. Paris, **274**, 1972, A1145–1148.
Gras,G. [72c]: Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France, **100**, 1972, 177–193.
Gras,G. [73]: Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, Ann. Inst. Fourier, **23**, 1973, 177–190.
Gras,G. [74a]: Problémes relatifs aux l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, Bull. Soc. Math. France, Mém. **37**, 1974, 91–100.
Gras,G. [74b]: Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l à cloture galoisienne diédrale de degré $2l$, J. Math. Soc. Japan, **26**, 1974, 677–685.
Gras,G. [75]: Critére de parité du nombre de classes des extensions abéliennes réelles de Q de degré impair, Bull. Soc. Math. France, **103**, 1975, 177–190.
Gras,G. [77a]: Étude d'invariants relatifs aux groupes des classes de corps abéliens, Astérisque, **41/42**, 1977, 35–53.
Gras,G. [77b]: Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier, **27**, 1977, no.1, 1–66.
Gras,G. [78]: Nombre de ϕ-classes invariantes, application aux classes des corps abéliens, Bull. Soc. Math. France, **106**, 1978, 337–364.
Gras,G. [79a]: Sur l'annulation en 2 des classes relatives des corps abéliens, C.R. Math. Rep. Acad. Sci. Canada, **1**, 1979, 107–110.
Gras,G. [79b]: Annulation du groupe des l-classes généralisées d'une extension abélienne réelle de degré premier à l, Ann. Inst. Fourier, **29**, 1979, no.1, 15–32.
Gras,G. [89]: Relations congruentielles linéaires entre nombres de classes de corps quadratiques, Acta Arith., **52**, 1989, 147–162.
Gras,G. [94]: Classes généralisées invariantes, J. Math. Soc. Japan, **46**, 1994, 467–476.
Gras,G. [97]: Principalization d'idéaux par extensions absolutement abeliennes, J. Number Theory, **62**, 1997, 403–421.
Gras,G. [98]: Théorèmes de réflexion, J. Théor. Nombres Bordeaux, **10**, 1998, 399–499.
Gras,G. [03]: *Class Field Theory*, Springer 2003.
Gras,G.,Gras M.-N. [75]: Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de Q de degré premier impair, Ann. Inst. Fourier, **25**, 1975, no.1, 1–22.
Gras M.-N. [74]: Sur les corps cubiques cycliques dont l'anneau des entiers est monogène, C.R. Acad. Sci. Paris, **278**, 1974, 59–62.
Gras M.-N. [81]: Z-bases d'entiers $1, \theta, \theta^2, \theta^3$ dans les extensions cycliques de degré 4 de Q, Publ. Math. Fac. Sci. Besançon, 1979/1980 and 1980/1981, No.6, 1–14.
Gras,M.-N. [84]: Non monogènéité de l'anneau des entiers de certaines extensions abéliennes de Q, Publ. Math. Fac. Sci. Besançon, 1983/1984, No.5, 1–25.

Gras,M.-N. [86a]: Non monogènéité de l'anneau des entiers des extensions cycliques de Q de degré premier $l \geq 5$, J. Number Theory, **23**, 1986, 347–353.
Gras,M.-N. [86b]: Condition nécessaire de monogènéité de l'anneau des entiers d'une extensions abélienne de Q, Sém. Th. Nombres, Paris 1984–85, Progr. Math., **63**, 97–107, Birkhäuser 1986.
Gras,M.N.,Moser,C.,Payan,J.J. [73]: Approximation algorithmique du groupe des classes de certains corps cubiques cycliques, Acta Arith., **23**, 1973, 295–300.
Gras,M.-N.,Tanoé,F. [95]: Corps biquadratiques monogènes, Manuscripta Math., **86**, 1995, 63–79.
Greaves,A.,Odoni,R.W.K. [88]: Weil numbers and CM-fields, I, J. Reine Angew. Math., **391**, 1988, 198–212.
Grebenyuk,D.G. [58]: On the theory of algebraic integers depending on a root of an irreducible equation of fourth degree, IAN Uzbek. SSR, 1958, nr.6, 27–47 (Russian).
Greenberg,M.J. [74]: An elementary proof of the Kronecker-Weber theorem, Amer. Math. Monthly, **81**, 1974, 601–607; corr.: **82**, 1975, p.803.
Greenberg,R. [73a]: A generalization of Kummer's criterion, Invent. math., **21**, 1973, 247–254.
Greenberg,R. [73b]: The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. Math., **95**, 1973, 204–214.
Greenberg,R. [75]: On p-adic L-functions and cyclotomic fields, Nagoya Math. J., **56**, 1975, 61–77; II, **67**, 1977, 139–158.
Greenberg,R. [76]: On the Iwasawa invariants of totally real number fields, Amer. J. Math., **98**, 1976, 263–284.
Greenberg,R. [78]: On 2-adic L-functions and cyclotomic invariants, Math. Z., **159**, 1978, 37–45.
Greenberg,R. [85]: On the critical values of Hecke L-functions for imaginary quadratic fields, Invent. math., **79**, 1985, 79–94.
Greenberg,R. [87]: Nonvanishing of certain values of L-functions, in: *Analytic Number Theory and Diophantine Problems (Stillwater 1984)*, 223–235, Progr. Math., **70**, Birkhäuser 1987.
Greenberg,R. [01]: Iwasawa theory - past and present, in: *Class Field Theory – its Centenary and Prospect (Tokyo 1998)*, 335–385, Tokyo 2001.
Greiman,G.,Geroldinger,A. [00]: An addition theorem and its arithmetical application, J. Number Theory, **85**, 2000, 59–73.
Greiter,G. [78]: A simple proof of a theorem of Kronecker, Amer. Math. Monthly, **85**, 1978, 756–757.
Greiter,G. [80]: Explizite Formeln für Einheiten algebraischer Zahlkörper und eine Familie irreduzibler Polynome über Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, **50**, 1980, 157–161.
Greither,C. [90]: Relative integral normal bases in $Q(\zeta_p)$, J. Number Theory, **35**, 1990, 180–193.
Greither,C. [96]: On Chinburg's second conjecture for abelian fields, J. Reine Angew. Math., **479**, 1996, 1–37.
Greither,C. [97]: On normal integral bases in ray class fields over imaginary quadratic fields, Acta Arith., **78**, 1997, 315–329.
Greither,S. [98]: The structure of some minus class groups, and Chinburg's third conjecture for abelian fields, Math. Z., **229**, 1998, 107–136.
Greither,C. [00]: Galois-Cohen-Lenstra, Acta Math. Inform. Univ. Ostraviensis, **8**, 2000, 33–43.
Greither,C.,Hachami,S.,Kučera,R. [01]: Racines d'unités cyclotomiques et divisibilité du nombre de classes d'un corps abélien réel, Acta Arith., **96**, 2001, 247–259.

Greither,C.,Rubin,K.,Srivastav,A. [99]: Swan modules and Hilbert–Speiser number fields, J. Number Theory, 79, **1999**, 164–173.
Grell,H. [27]: Zur Theorie der Ordnungen in algebraischen Zahl- und Funktionenkörpern, Math. Ann., **97**, 1927, 524–558.
Grell,H. [36a]: Über die Gültigkeit der gewöhnlichen Idealtheorie in endlichen algebraischen Erweiterungen erster und zweiter Art, Math. Z., **40**, 1936, 503–505.
Grell,H. [36b]: Verzweigungstheorie in allgemeinen Ordnungen algebraischer Zahlkörper, Math. Z., **40**, 1935, 629–657.
Gronwall,T.H. [13]: Sur les séries de Dirichlet correspondant à des caractéres complexes, Rend. Circ. Mat. Palermo, **35**, 1913, 145–159.
Gross,B.H. [80]: *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Math., **776**, Springer 1980.
Gross,B.,Zagier,D. [83]: Points de Heegner et dérivées de fonctions L, C.R. Acad. Sci. Paris, **297**, 1983, 85–87.
Gross,B.,Zagier,D. [86]: Heegner points and the derivatives of L-series, Invent. math., **84**, 1986, 225–320.
Grossman,E.H. [76]: On the solutions of diophantine equations in units, Acta Arith., **30**, 1976, 137–143.
Grossman,E.H. [77]: Sums of roots of unity in cyclotomic fields, J. Number Theory, **9**, 1977, 321–329.
Grosswald,E. [63]: Negative discriminants of binary quadratic forms with one class in each genus, Acta Arith., **8**, 1963, 295–306.
Grosswald,E. [66]: L-functions and quadratic fields with unique factorization, Duke Math. J., **33**, 1966, 169–185.
Grotz,W. [80]: Einige Anwendungen der Siegelschen Summenformel, Acta Arith., **38**, 1980, 69–95.
Grube,F. [74]: Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen, Zeitschr. Math. Phys., (5) **19**, 1874, 492–519.
Gruenberg,K.W.,Weiss,A. [00]: Capitulation and transfer kernels, J. Théor. Nombres Bordeaux, **12**, 2000, 219–226.
Grundman,H.G. [95]: Systems of fundamental units in cubic orders, J. Number Theory, **50**, 1995, 119–127.
Grunwald,W. [33]: Ein allgemeines Existenztheorem für algebraische Zahlkörper, J. Reine Angew. Math., **169**, 1933, 103–107.
Guého,M.F. [72a]: Corps de quaternions et fonctions zêta au point -1, C.R. Acad. Sci. Paris, **274**, 1972, A296–298.
Guého,M.F. [72b]: *Corps de quaternions sur un corps de nombres algébriques*, Thése, Univ. Bordeaux I, 1972.
Guého,M.F. [74a]: Le théorème d'Eichler sur le nombre de classes d'idéaux d'un corps de quaternions totalement défini et la mesure de Tamagawa, Bull. Soc. Math. France, Mém. **37**, 1974, 107–114.
Guého,M.F. [74b]: Sur les corps de quaternions, Publ. Math. Univ. Bordeaux, 1973/74, no.1, 35–56.
Guerrier,W.J. [68]: The factorization of the cyclotomic polynomial mod p, Amer. Math. Monthly, **75**, 1968, p.46.
Gundlach,K.-B. [73]: Die Berechnung von Zetafunktionen mit Vorzeichencharakter an der Stelle l, Acta Arith., **24**, 1973, 201–221.
Gupta,R.,Murty M.R.,Murty,V.K. [87]: The Euclidean algorithm for S-integers, in: *Number Theory (Montreal, 1985)*, 189–201, Amer. Math. Soc. 1987.
Gurak,S. [78a]: On the Hasse norm principle, J. Reine Angew. Math., **299/300**, 1978, 16–27.
Gurak,S. [78b]: The Hasse norm principle in non-abelian extensions, J. Reine Angew. Math., **303/304**, 1978, 314–318.

Gurak,S. [80]: The Hasse norm principle in a compositum of radical extensions, J. London Math. Soc., (2) **22**, 1980, 385–397.
Gurak,S. [82]: Minimal polynomials for Gauss circulants and cyclotomic units, Pacific J. Math., **102**, 1982, 347–353.
Guralnick,R.M.,Stern,L. [95]: Solitary Galois extensions of algebraic number fields, J. Number Theory, **50**, 1995, 1–32.
Gurevich,M.M. [71]: On the determination of L-series by their functional equation, Mat. Sb., **85**, 1971, 538–552. (Russian)
Gut,M. [29]: Die Zeta-Funktion, die Klassenzahl und die Kroneckersche Grenzformel eines beliebigen Kreiskörpers, Comment. Math. Helv., **1**, 1929, 160–226.
Gut,M. [32]: Über die Primidealzerlegung in gewisser relativ-ikosaedrischen Zahlkörpern, Comment. Math. Helv., **4**, 1932, 219–229.
Gut,M. [33]: Weitere Untersuchungen über die Primidealzerlegung in gewisser relativ-ikosaedrischen Zahlkörpern, Comment. Math. Helv., **6**, 1933, 47–75.
Gut,M. [37]: Über Erweiterungen von unendlichen algebraischen Zahlkörper, Comment. Math. Helv., **9**, 1937, 136–155.
Gut,M. [43a]: Zur Theorie der Strahlklassenkörper der quadratisch reellen Zahlkörper, Comment. Math. Helv., **15**, 1943, 37–59.
Gut,M. [43b]: Zur Theorie der Kreiskörper, insbesondere der Strahlklassenkörper der quadratisch imaginären Zahlkörper, Comment. Math. Helv., **15**, 1943, 81–119.
Gut,M. [51a]: Eulersche Zahlen und Klassenzahl des Körpers der $4l$-ten Einheitswurzeln, Comment. Math. Helv., **25**, 1951, 43–63.
Gut,M. [51b]: Kubische Klassenkörper über quadratisch-imaginären Grundkörpern, Nieuw Arch. Wisk., (2) **23**, 1951, 185–189.
Gut,M. [54]: Relativquadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teilbar sind, Comment. Math. Helv., **28**, 1954, 270–277.
Gut,M. [73]: Erweiterungskörper von Primzahlgrad mit durch diese Primzahl teilbarer Klassenzahl, Enseign. Math., **19**, 1973, 119–123.
Gut,M.,Stünzi,M. [66]: Kongruenzen zwischen Koeffizienten trigonometrischen Reihen und Klassenzahlen quadratisch imaginärer Körper, Comment. Math. Helv., **41**, 1966/67, 287–302.
Güting,R. [77]: Positive inverse Einheiten in komplexen kubischen Zahlkörpern, Acta Arith., **34**, 1977/78, 1–7.
Győry,K. [73]: Sur les pôlynomes à coefficients entiérs et de discriminant donné, Acta Arith., **23**, 1973, 419–426; II, Publ. Math. Debrecen, **21**, 1974, 125–144; III, **23**, 1976, 141–165; IV, **25**, 1978, 155–167; V, Acta Math. Acad. Sci. Hungar., **31**, 1978, 175–190.
Győry,K. [75]: Sur une classe des corps de nombres algébriques et ses applications, Publ. Math. Debrecen, **22**, 1975, 151–175.
Győry,K. [79a]: Corps de nombres algébriques d'anneau d'entiers monogène, Sém. DPP, **20**, 1978/79, fasc.2, exp.26.
Győry,K. [79b]: On the number of solutions of linear equations in units of an algebraic number field, Comment. Math. Helv., **54**, 1979, 583–600.
Győry,K. [80a]: Explicit upper bounds for the solutions of some diophantine equations, Ann. Acad. Sci. Fenn. Ser. A1, **5**, 1980, 3–12.
Győry,K. [80b]: On certain graphs composed of algebraic integers of a number field and their applications, I, Publ. Math. Debrecen, **27**, 1980, 229–242.
Győry,K. [81a]: On S-integral solutions of norm form, discriminant form and index form equations, Studia Sci. Math. Hungar., **16**, 1981, 149–161.
Győry,K. [81b]: On discriminants and indices of integers of an algebraic number field, J. Reine Angew. Math., **324**, 1981, 114–126.

Győry,K. [83]: Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, Acta Math. Acad. Sci. Hungar., **42**, 1983, 45–80.
Győry,K. [84]: Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely [generated] domains, J. Reine Angew. Math., **346**, 1984, 54–100; corr. **347**, 1984, p.167.
Győry,K. [95]: On a problem of A.M.Odlyzko on algebraic units of bounded degree, Acta Math. Acad. Sci. Hungar., **69**, 1995, 1–4.
Győry,K. [98a]: Bounds for the solutions of decomposable form equations, Publ. Math. Debrecen, **52**, 1998, 1–31.
Győry,K. [98b]: Recent bounds for the solutions of decomposable form equations, in: *Number Theory*, 255–270, de Gruyter 1998.
Győry,K. [99]: On the distribution of solutions of decomposable form equations, in: *Number Theory in Progress*, **I**, 237–265, de Gruyter 1999.
Győry,K. [00]: Discriminant form and index form equations, in: *Algebraic Number Theory and Diophantine Analysis*, (Graz 1998), 191–214, de Gruyter 2000.
Győry,K.,Papp,Z.Z. [77]: On discriminant form and index form equations, Studia Sci. Math. Hungar., **12**, 1977, 47–60.
Győry,K.,Papp,Z.Z. [78]: Effective estimates for the integer solutions of norm form and discriminant form equations, Publ. Math. Debrecen, **25**, 1978, 311–325.
Győry,K.,Papp,Z.Z. [83]: Norm form equations and explicit lower bounds for linear forms with algebraic coefficients, *Studies in Pure Mathematics*, 245–257, Birkhäuser 1983.
Győry,K.,Pethő,A. [75]: Sur la distribution des solutions des équations du type "norme-forme", Acta Math. Acad. Sci. Hungar., **26**, 1975, 135–142.
Győry,K.,Pethő,A. [77]: Über die Verteilung der Lösungen von Normformen Gleichungen, II, Acta Arith., **32**, 1977, 349–363; III, **37**, 1980, 143–165.
Haberland,K. [74]: Über die Anzahl der Erweiterungen eines algebraischen Zahlkörpers mit einer gegebener abelscher Gruppe als Galoisgruppe, Acta Arith., **26**, 1974, 153–158.
Hafner,J.L. [83]: The distribution and average order of the coefficients of Dedekind ζ functions, J. Number Theory, **17**, 1983, 183–190.
Haggenmüller,R. [82]: Signaturen von Einheiten und unverzweigte quadratische Erweiterungen total-reeller Zahlkörper, Archiv Math., **39**, 1982, 312–321.
Hajir,F. [96]: On a theorem of Koch, Pacific J. Math., **176**, 1996, 15–18.
Hajir,F. [97a]: On the growth of p-class groups in p-class field towers, J. Algebra, **188**, 1997, 256–271.
Hajir,F. [97b]: On the class numbers of Hilbert class fields, Pacific J. Math., Special Issue, 1997, 177–187.
Hajir,F.,Maire,C. [01]: Tamely ramified towers and discriminant bounds for number fields, Compositio Math., **128**, 2001, 35–53; II, J. Symbolic Comp., **33**, 2002, 415–423.
Hajir,F.,Maire,C. [02]: Unramified subextensions of ray class field towers, J. Algebra, **249**, 2002, 528–543.
Halbritter,U.,Pohst,M. [90]: On the computation of the values of zeta functions of totally real cubic fields, J. Number Theory, **36**, 1990, 266–288.
Hall,N.A. [37]: Binary quadratic forms with a single class of reduced forms in each genus, Proc. Nat. Acad. Sci. U.S.A., **23**, 1937, 414–415.
Hall,N.A. [39]: Binary quadratic discriminants with a single class of forms in each genus, Math. Z., **44**, 1939, 85–90.
Halter-Koch,F. [67]: Arithmetische Kennzeichnung der Spur des Einsdivisors, J. Reine Angew. Math., **228**, 1967, 217–219.

Halter-Koch,F. [71a]: Algebraische Zahlen mit Konjugierten auf dem Einheitskreis, Archiv Math., **22**, 1971, 161–164.
Halter-Koch,F. [71b]: Arithmetische Theorie der Normalkörper vom 2-Potenzgrad mit Diedergruppe, J. Number Theory, **3**, 1971, 412–443.
Halter-Koch,F. [71c]: Geschlechtertheorie der Ringklassenkörper, J. Reine Angew. Math., **250**, 1971, 107–108.
Halter-Koch,F. [72a]: Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern, J. Number Theory, **4**, 1972, 70–77.
Halter-Koch,F. [72b]: Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Körper, J. Number Theory, **4**, 1972, 144–156.
Halter-Koch,F. [75]: Unabhängige Einheitensysteme für eine allgemeine Klasse algebraischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **43**, 1975. 85–91.
Halter-Koch,F. [77]: Einheiten und Divisorenklassen in Galois'schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl l, Acta Arith., **33**, 1977, 353–364.
Halter-Koch,F. [78a]: Die Struktur der Einheitengruppe für eine Klasse metazyklischer Erweiterungen algebraischer Zahlkörper, J. Reine Angew. Math., **301**, 1978, 147–160.
Halter-Koch,F. [78b]: Eine allgemeine Geschlechtertheorie und ihre Anwendung auf Teilbarkeitsaussagen für Klassenzahlen algebraischer Zahlkörper, Math. Ann., **233**, 1978, 55–63.
Halter-Koch,F. [78c]: Über den p-Rang der Klassengruppe des Kompositums algebraischer Zahlkörper, Math. Ann., **238**, 1978, 119–122.
Halter-Koch,F. [80]: Über Radikalerweiterungen, Acta Arith., **36**, 1980, 43–58.
Halter-Koch,F. [81]: Grosse Faktoren in der Klassengruppe algebraischer Zahlkörper, Acta Arith., **39**, 1981, 33–47.
Halter-Koch,F. [82]: Metrische Theorie der Einheiten algebraischer Zahlkörper, Mitt. Math. Ges. Hamburg, **11**, 1982, 131–141.
Halter-Koch,F. [83]: Factorization of algebraic integers, Ber. Math. Stat. Sektion, Graz, **191**, 1983, 1–24.
Halter-Koch,F. [84a]: Über den 4-Rang der Klassengruppe quadratischer Zahlkörper, J. Number Theory, **19**, 1984, 219–227.
Halter-Koch,F. [84b]: On the factorization of algebraic integers into irreducibles, in: *Topics in Classical Number Theory*, 699–707, North-Holland 1984.
Halter-Koch,F. [89]: Reell-quadratische Zahlkörper mit großer Grundeinheit, Abh. Math. Sem. Univ. Hamburg, **59**, 1989, 171–181.
Halter-Koch,F. [90a]: Quadratische Ordnungen mit grosser Klassenzahl, J. Number Theory, **34**, 1990, 82–94; II, **44**, 1993, 166–171.
Halter-Koch,F. [90b]: Halbgruppen mit Divisorentheorie, Exposition Math., **8**, 1990, 27–66.
Halter-Koch,F. [91]: Prime-producing quadratic polynomials and class numbers of quadratic orders, in: *Computational Number Theory (Debrecen 1989)*, 73–82, de Gruyter 1991.
Halter-Koch,F. [92a]: A generalization of Davenport's constant and its arithmetical applications, Colloq. Math., **63**, 1999, 203–210.
Halter-Koch,F. [92b]: Chebotarev formations and quantitative aspects of non-unique factorizations, Acta Arith., **62**, 1992, 173–206.
Halter-Koch,F. [92c]: Typenhalbgruppen und Faktorisierungsprobleme, Results in Math., **22**, 1992, 545–559.
Halter-Koch,F. [92d]: Relative types and their arithmetical applications, Pure Math. Appl., **A3**, 1992, 81–92.

Halter-Koch,F. [92e]: Relative block semigroups and their arithmetical applications, Comment. Math. Univ. Carolin., **33**, 1992, 373–381.

Halter-Koch,F. [93a]: Über Längen nicht-eindeutiger Faktorisierungen und Systeme linearer diophantischer Ungleichungen, Abh. Math. Sem. Univ. Hamburg, **63**, 1993, 265–276.

Halter-Koch,F. [93b]: Factorization problems in class number two, Colloq. Math., **65**, 1993, 255–265.

Halter-Koch,F. [93c]: On the asymptotic behaviour of the number of distinct factorizations into irreducibles, Ark. Mat., **31**, 1993, 297–305.

Halter-Koch,F. [95]: Elasticity of factorizations in atomic monoids and integral domains, J. Théor. Nombres Bordeaux, **7**, 1995, 367–385.

Halter-Koch,F.,Lorenz,F. [81]: Ein Normalbasissatz für Einheiten algebraischer Zahlkörper, Math. Ann., **257**, 1981, 335–339.

Halter-Koch,F.,Moser,N. [78]: Sur le nombre de classes de certaines extensions métacycliques sur Q ou sur un corps quadratique imaginaire, J. Math. Soc. Japan, **30**, 1978, 237–248.

Halter-Koch,F.,Müller,W. [91]: Quantitative aspects of non-unique factorization: a general theory with applications to algebraic functions fields, J. Reine Angew. Math., **421**, 1991, 159–188.

Halter-Koch,F.,Narkiewicz,W. [99]: Polynomial cycles and dynamical units, Proc. Conf. Analytic and Elementary Number Theory (Vienna 1996), 70–80, Wien, 1999.

Halter-Koch,F.,Narkiewicz,W. [00]: Scarcity of finite polynomial orbits, Publ. Math. Debrecen, **56**, 2000, 405–414.

Hamada,S. [83]: Norm theorem on splitting fields of some binomial polynomials, Kodai Math. J., **6**, 1983, 47–50.

Hamamura,M. [81]: On absolute class fields of certain algebraic number fields, Natur. Sci. Rep. Ochanomizu Univ., **32**, 1981, 23–34.

Haneke,W. [69]: Darstellung von Primzahlen durch quadratische Formen, Math. Z., **110**, 1969, 10–14.

Haneke,W. [73]: Über die reellen Nullstellen der Dirichletschen L-Reihen, Acta Arith., **22**, 1973, 391–421; corr., **31**, 1976, 99–100.

Hara,Y. [93]: On calculation of $L_K(1,\chi)$ for some Hecke characters, J. Math. Kyoto Univ., **33**, 865–898.

Haran,S. [90]: Riesz potentials and explicit sums in arithmetic, Invent. math., **101**, 1990, 697–703.

Harder,G.,Pink,R. [92]: Modular konstruierte unverzweigte abelsche p-Erweiterungen von $Q(\zeta_p)$ und die Struktur ihrer Galoisgruppen, Math. Nachr., **159**, 1992, 83-99.

Hardy,G.H. [19]: A problem of diophantine approximation, J. Indian Math. Soc., **11**, 1919, 162–166.

Hardy,G.H.,Littlewood,J.E. [23]: The approximate functional equation in the theory of zeta-function with application to the divisor problems of Dirichlet and Piltz, Proc. London Math. Soc., (2) **21**, 1923, 39–74.

Hardy,G.H.,Wright,E.M. [60]: *An Introduction to the Theory of Numbers*, Oxford 1938, 4th ed. 1960.

Hardy,K.,Hudson,R.H.,Richman,D.R.,Williams,K.S. [89]: Determination of all imaginary cyclic quartic fields with class number 2, Trans. Amer. Math. Soc., **311**, 1989, 1–55.

Hardy,K.,Hudson,R.H.,Richman,D.R.,Williams,K.S.,Holtz,N.M. [86]: *Calculation of the Class Numbers of Imaginary Cyclic Quartic fields*, Carleton–Ottawa Math. Lecture Note Series, Nr. 7, 1986.

Hardy,K.,Hudson,R.H.,Richman,D.R.,Williams,K.S.,Holtz,N.M. [87]: Calculation of the class numbers of imaginary cyclic quartic fields, Math. Comp., **49**, 1987, 615–620.

Harris,M.,Taylor,R. [01]: *The Geometry and Cohomology of some Simple Shimura Varieties*, Ann. of Math.Studies, **151**, Princeton 2001.

Hartung,P. [74a]: Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, J. Number Theory, **6**, 1974, 276–278.

Hartung,P. [74b]: Explicit construction of a class of infinitely many imaginary quadratic fields whose class number is divisible by 3, J. Number Theory, **6**, 1974, 279–281.

Haselgrove,C.B. [51]: Some theorems in the analytic theory of numbers, J. London Math. Soc., **26**, 1951, 273–277.

Hasse,H. [23a]: Über die Darstellbarkeit der Zahlen durch quadratische Formen im Körper der rationalen Zahlen, J. Reine Angew. Math., **152**, 1923, 129–148.

Hasse,H. [23b]: Über Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, J. Reine Angew. Math., **152**, 1923, 205–224.

Hasse,H. [24a]: Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, J. Reine Angew. Math., **153**, 1924, 113–130.

Hasse,H. [24b]: Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, J. Reine Angew. Math., **153**, 1924, 158–162.

Hasse,H. [26a]: Zwei Existenztheoreme über algebraische Zahlkörper, Math. Ann., **95**, 1926, 229–238.

Hasse,H. [26b]: Ein weiteres Existenztheorem in der Theorie der algebraischen Zahlkörper, Math. Z., **24**, 1926, 149–160.

Hasse,H. [26c]: *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein., **35**, 1926, 1–55; **36**, 1927, 233–311; **VI** Erg.Bd., 1930. [Reprint: Wien 1965, 1970.]

Hasse,H. [27]: Neue Begründung der komplexen Multiplikation, J. Reine Angew. Math., **157**, 1927, 115–139; **165**, 1931, 64–88.

Hasse,H. [28]: Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen, J. Reine Angew. Math., **159**, 1928, 3–12.

Hasse,H. [30a]: Ein Satz über relativ-Galoische Zahlkörper und seine Anwendung auf relativ-Abelsche Zahlkörper, Math. Z., **31**, 1930, 559–564.

Hasse,H. [30b]: Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischen Grundlage, Math. Z., **31**, 1930, 559–564.

Hasse,H. [30c]: Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper, J. Reine Angew. Math., **162**, 1930, 169–184.

Hasse,H. [31d]: Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachr. Ges. Wiss. Göttingen, 1931, 64–69.

Hasse,H. [32]: Zwei Bemerkungen zu der Arbeit "Zur Arithmetik der Polynome" von U.Wegner in den Math. Ann. 105, S. 628–631, Math. Ann., **106**, 1932, 455–456.

Hasse,H. [33]: Explizite Konstruktion zyklischer Klassenkörper, Math. Ann., **109**, 1933, 191–195.

Hasse,H. [34]: Normenresttheorie Galoischer Zahlkörper mit Anwendungen auf Führer und Diskriminante algebraischer Zahlkörper, J. Fac. Sci. Univ. Tokyo, **2**, 1934, 477–498.

Hasse,H. [37]: Über die Diskriminante auflösbarer Körper mit Primzahlgrad, J. Reine Angew. Math., **176**, 1937, 12–17.

Hasse,H. [40]: Produktformeln für verallgemeinerte Gausssche Summen und ihre Anwendungen auf die Klassenzahlformeln für reelle quadratische Zahlkörper, Math. Z., **46**, 1940, 303–314.

Hasse,H. [48a]: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Abhandl. Deutsch. Akad. Wiss., 1948, No.2, 3–95.

Hasse,H. [48b]: Die Einheitengruppe in einem total-reellen nichtzyklischen kubischen Zahlkörper und in zugehörigen bikubischen Normalkörper, Archiv Math., **1**, 1948, 42–46; Miscel. Acad. Berol., **1**, 1950, 1–24.

Hasse,H. [49]: *Zahlentheorie*, Akademie–Verlag 1949; 2nd ed. 1963, 3rd ed. 1969. [English translation: Springer 1980; reprint: Springer 2002].

Hasse,H. [50a]: *Vorlesungen über Zahlentheorie*, Springer 1950; 2nd ed. 1964.

Hasse,H. [50b]: Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine Angew. Math., **188**, 1950, 40–64.

Hasse,H. [51a]: Allgemeine Theorie der Gaussschen Summen in algebraischen Zahlkörpern, Abhandl. Deutsch. Akad. Wiss., 1951, No.1, 1–23.

Hasse,H. [51b]: Zur Geschlechtertheorie in quadratischen Zahlkörpern, J. Math. Soc. Japan, **3**, 1951, 45–51.

Hasse,H. [51c]: Über das Problem der Primzerlegung in Galoisschen Zahlkörpern, S.-B. Berliner Math. Ges., 1951/52, 8–27.

Hasse,H. [52a]: *Über die Klassenzahl Abelscher Zahlkörper*, Berlin 1952. [Reprint: Akademie Verlag 1985.]

Hasse,H. [52b]: Gausssche Summen zu Normalkörpern über endlich-algebraischen Zahlkörpern, Abhandl. Deutsch. Akad. Wiss., 1952, No.1, 1–19.

Hasse,H. [54a]: Artinsche Führer, Artinsche L-Funktionen und Gaussschen Summen über endlich-algebraischen Zahlkörpern, Acta Salamant., Math., **4**, 1954, 1–113.

Hasse,H. [54b]: Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abhandl. Deutsch. Akad. Wiss., 1954, no.4, 5–70.

Hasse,H. [55]: Die dyadische Einseinheitenoperatorengruppe zum Körper der 2^n-ten Einheitswurzeln nebst Anwendung auf die Klassenzahl seines grössten reellen Teilkörpers, Rev. Fac. Sci. Univ. Istanbul, **20**, 1955, 7–126.

Hasse,H. [62]: Kurt Hensels entscheidender Anstoss zur Entdeckung des Lokal-Global Prinzips. J. Reine Angew. Math., **209**, 1962, 3–4.

Hasse,H. [64]: Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47, Acta Arith., **9**, 1964, 419–434.

Hasse,H. [66]: Vandiver's congruence for the relative class number of the p-th cyclotomic field, J. Math. Anal. Apl., **15**, 1966, 87–90.

Hasse,H. [67]: *Vorlesungen über Klassenkörpertheorie*, Würzburg 1967.

Hasse,H. [69a]: Eine Folgerung aus H.-W.Leopoldts Theorie der Geschlechter abelscher Zahlkörper, Math. Nachr., **42**, 1969, 261–262.

Hasse,H. [69b]: Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, J. Number Theory, **1**, 1969, 231–234.

Hasse,H. [69c]: Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \pmod{2^3}$, Aequat. Math., **3**, 1969, 165–169.

Hasse,H. [69d]: Eine Folgerung aus H.-W.Leopoldt's Theorie der Geschlechter abelscher Zahlkörper, Math. Nachr., **42**, 1969, 261–262.

Hasse,H. [70a]: Über die Teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math., **241**, 1970, 1–6.

Hasse,H. [70b]: Über Teilbarkeit durch 2^3 der Klassenzahl quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, Math. Nachr., **46**, 1970, 61–70.

Hasse,H.,Hensel,K. [23]: Über die Normenreste eines relativ-zyklischen Körpers vom Primzahlgrad l nach einem Primteiler $\mathfrak{L}$ von l, Math. Ann., **90**, 1923, 262–278.

Hasse,H.,Liang,J. [69]: Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47 (Fortsetzung), Acta Arith., **16**, 1969, 89–97.

Hasse,H.,Schmidt,F.K. [33]: Die Struktur diskret bewerteter Körper, J. Reine Angew. Math., **170**, 1933, 4–63.

Hasse,H.,Suetuna,Z. [31]: Ein allgemeines Teilerproblem der Idealtheorie, J. Fac. Sci. Univ. Tokyo, **2**, 1931, 133–154.

Hassler,W. [03]: A note on half-factorial set of finite cyclic groups, Far East J. Math. Sci., **10**, 2003, 187–198.

Haugland,J.K. [95]: A walk on complex primes, Normat, **43**, 1995, 168–170. (Norwegian)

Hayashi,H. [77]: Note on the class numbers of the quadratic number fields $Q(\sqrt{-p})$, $Q(\sqrt{-2p})$ and $Q(\sqrt{2p})$ with a prime number $p \equiv 1 \pmod{2^2}$, Mem. Fac. Gen. Ed. Kumamoto Univ., **13**, 1977, 1–8.

Hayashi,Y. [88]: Reelle biquadratische Zahlkörper mit ungerader Klassenzahl, Manuscripta Math., **62**, 1988, 65–82.

Hayes,D.R. [74]: Explicit class field theory for rational function fields, Trans. Amer. Math. Soc., **189**, 1974, 77–91.

Hayes,D.R. [79]: Explicit class field theory in global function fields, in: *Studies in Algebra and Number Theory*, 173–217, New York 1979,

Hayes,D.R. [90]: The partial zeta functions of a real quadratic field evaluated at $s = 0$, in: *Number Theory (Banff 1988)*, 207–226, de Gruyter 1990.

Hays,J.H. [73]: Reduction of ideals in commutative rings, Trans. Amer. Math. Soc., **177**, 1973, 51–63.

Hazama,F. [90]: Demjanenko matrix, class numbers, and Hodge group, J. Number Theory, **34**, 1990, 174–177.

Hazewinkel,M. [69]: *Abelian Extensions of Local Fields*, Groningen 1969.

Hazewinkel,M. [75]: Local class field theory is easy, Adv. in Math., **18**, 1975, 148–181.

Heath-Brown,D.R. [77]: On the density of the zeros of the Dedekind zeta-function, Acta Arith., **33**, 1977, 169–181.

Heath-Brown,D.R. [79]: On a paper of Baker and Schinzel, Acta Arith., **35**, 1979, 203–207.

Heath-Brown,D.R. [88]: The growth rate of the Dedekind zeta-function on the critical line, Acta Arith., **49**, 1988, 323–339.

Heath-Brown,D.R.,Patterson,S.J. [79]: The distribution of Kummer sums at prime arguments, J. Reine Angew. Math., **310**, 1979, 111–130.

Hecke,E. [10]: Über nicht-reguläre Primzahlen und den Fermatschen Satz, Nachr. Ges. Wiss. Göttingen,1910, 420–424 = *Mathematische Werke*, 59–63, Göttingen 1959.

Hecke,E. [12]: Zur Theorie der Modulfunktionen von zwei Variablen und ihre Anwendung auf die Zahlentheorie, Math. Ann., **71**, 1912, 1–37 = *Mathematische Werke*, 21–57, Göttingen 1959.

Hecke,E. [13]: Über die Konstruktion relativ-abelscher Zahlkörper durch Modulfunktionen von zwei Variablen, Math. Ann., **74**, 1913, 465–510 = *Mathematische Werke*, 69–114, Göttingen 1959.

Hecke,E. [17a]: Über die Zetafunktion beliebiger algebraischer Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1917, 77–89 = *Mathematische Werke*, 159–171, Göttingen 1959.

Hecke,E. [17b]: Über eine neue Anwendung der Zetafunktion auf die Arithmetik der Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1917, 90–95 = *Mathematische Werke*, 215–234, Göttingen 1959.

Hecke,E. [17c]: Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1917, 299–318 = *Mathematische Werke*, 178–197, Göttingen 1959.

Hecke,E. [17d]: Über die Kroneckersche Grenzformel für reelle quadratische Körper und die Klassenzahl relativ-abelscher Körper, Verh. Naturforsch. Ges. Basel, **28**, 1917, 363–372 = *Mathematische Werke*, 198–207, Göttingen 1959.

Hecke,E. [18]: Eine neue Art von Zetafunktionen und ihre Beziehung zur Verteilung der Primzahlen, Math. Z., **1**, 1918, 357–376; II, **6**, 1920, 11–51 = *Mathematische Werke*, 215–234, 249–289, Göttingen 1959.

Hecke,E. [19]: Reziprozitätsgesetz und Gausssche Summen in quadratischen Zahlkörpern, Nachr. Ges. Wiss. Göttingen, 1919, 265–278 = *Mathematische Werke*, 235–248, Göttingen 1959.

Hecke,E. [21a]: Analytische Funktionen und algebraische Zahlen, Abh. Math. Sem. Univ. Hamburg, **1**, 1921, 102–126; II, **3**, 1924, 213–236 = *Mathematische Werke*, 213–236, Göttingen 1959.

Hecke,E. [21b]: Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern, Nachr. Ges. Wiss. Göttingen, 1921, 1–23 = *Mathematische Werke*, 290–312, Göttingen 1959.

Hecke,E. [23]: *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923; 2nd ed. 1954. [Reprint: Chelsea 1970.]

Hecke,E. [25]: Darstellung der Klassenzahlen als Perioden von Integralen 3 Gattung aus dem Gebiet der elliptischen Modulfunktionen, Abh. Math. Sem. Univ. Hamburg, **4**, 1925, 211–223 = *Mathematische Werke*, 405–417, Göttingen 1959.

Hecke,E. [30]: Über das Verhalten der Integrale 1 Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen, Abh. Math. Sem. Univ. Hamburg, **8**, 1930, 271–281 = *Mathematische Werke*, 548–558, Göttingen 1959.

Hecke,E. [37]: Über Dirichlet-Reihen mit Funktionalgleichung und ihre Nullstellen auf der Mittelgeraden, S.-B. Bayer. Akad. Wiss., 1937, 73–95 = *Mathematische Werke*, 708–730, Göttingen 1959.

Hecke,E. [39]: Die Klassenzahl imaginär-quadratischer Körper in der Theorie der elliptischen Modulfunktionen, Monatsh. Math. Phys., **48**, 1939, 75–83 = *Mathematische Werke*, 773–781, Göttingen 1959.

Heegner,H. [52]: Diophantische Analysis und Modulfunktionen, Math. Z., **56**, 1952, 227–253.

Heider,F.P. [80]: Strahlknoten und Geschlechterkörper mod m, J. Reine Angew. Math., **320**, 1980, 52–67.

Heider,F.P. [81]: Zahlentheoretische Knoten unendlicher Erweiterungen, Archiv Math., **37**, 1981, 341–352.

Heider,F.P. [84]: Kapitulationsprobleme und Knotentheorie, Manuscripta Math., **46**, 1984, 229–272.

Heider,F.P.,Schmithals,B. [82]: Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen, J. Reine Angew. Math., **336**, 1982, 1–25.

Heilbronn,H. [34]: On the class-number in imaginary quadratic fields, Quart. J. Math., Oxford ser., **5**, 1934, 150–160.

Heilbronn,H. [37]: On real characters, Acta Arith., **2**, 1937, 212–213.

Heilbronn,H. [38a]: On Euclid's algorithm in real quadratic fields, Proc. Cambridge Philos. Soc., **34**, 1938, 521–526.

Heilbronn,H. [38b]: On Dirichlet series which satisfy a certain functional equation, Quart. J. Math., Oxford ser., **9**, 1938, 194–195.

Heilbronn,H. [50]: On Euclid's algorithm in cubic self-conjugated fields, Proc. Cambridge Philos. Soc., **46**, 1950, 377–382.

Heilbronn,H. [51]: On Euclid's algorithm in cyclic fields, Canad. J. Math., **3**, 1951, 257–268.
Heilbronn,H. [67]: Zeta functions and L-functions, in: Cassels, Fröhlich [67], 204–230.
Heilbronn,H. [72]: On real simple zeros of Dedekind ζ-functions, Proc. Number Theory Conf., Boulder 1972, 108–110.
Heilbronn,H. [73]: On real simple zeros of Dedekind ζ-functions, Canad. J. Math., **25**, 1973, 870–873.
Heilbronn,H.,Linfoot,E.H. [34]: On the imaginary quadratic corpora of class-number one, Quart. J. Math., Oxford ser., **5**, 1934, 293–301.
Hendy,M.D. [74a]: Applications of a continued fraction algorithm to some class number problems, Math. Comp., **28**, 1974, 267–277.
Hendy,M.D. [74b]: Prime quadratics associated with complex quadratic fields of class number two, Proc. Amer. Math. Soc., **43**, 1974, 253–260.
Henniart,G.M. [00]: Une preuve simple des conjectures de Langlands pour $GL(n)$ sur un corps p-adique, Invent. math., **130**, 2000, 439–455.
Hensel,K. [84]: *Arithmetische Untersuchungen über Discriminanten und ihre ausserwesentliche Theiler*, Dissertation, Berlin 1884.
Hensel,K. [87]: Untersuchungen der ganzen algebraischen Zahlen eines gegebenes Gattungsbereiches für einen beliebigen algebraischen Zahlkörper, J. Reine Angew. Math., **101**, 1887, 99–141.
Hensel,K. [89]: Ueber Gattungen, welche durch Composition aus zwei anderen Gattungen entstehen, J. Reine Angew. Math., **105**, 1889, 329–344.
Hensel,K. [93]: Über die Darstellung der Determinante eines Systems welches aus zwei anderen componiert ist, Acta Math., **14**, 1893, 317–319.
Hensel,K. [94a]: Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante, J. Reine Angew. Math., **113**, 1894, 61–83.
Hensel,K. [94b]: Arithmetische Untersuchungen über die gemeinsamen Discriminantentheiler einer Gattung, J. Reine Angew. Math., **113**, 1894, 128–160.
Hensel,K. [97a]: Ueber die Bestimmung der Discriminante eines algebraischen Körpers, Nachr. Ges. Wiss. Göttingen, 1897, 247–253.
Hensel,K. [97b]: Ueber die Fundamentalgleichung und die ausserwesentliche Discriminantentheiler eines algebraischen Körpers, Nachr. Ges. Wiss. Göttingen, 1897, 247–253.
Hensel,K. [97c]: Über eine neue Begründung der Theorie der algebraischen Zahlen, Jahresber. Deutsch. Math.-Verein., **6**, 1897, 83–88.
Hensel,K. [97d]: Ueber die Fundamentaltheiler algebraischer Gattungsbereichen, J. Reine Angew. Math., **117**, 1897, 333–345.
Hensel,K. [97e]: Ueber die Elementartheiler zweier Gattungen, von denen die eine unter der anderen enthalten ist, J. Reine Angew. Math., **117**, 1897, 346–355.
Hensel,K. [99]: Ueber diejenigen algebraischen Körper, welche aus zwei anderen componiert sind, J. Reine Angew. Math., **120**, 1899, 99–108.
Hensel,K. [02]: Ueber die Entwicklung von algebraischen Zahlen in Potenzreihen, Math. Ann., **55**, 1902, 305–336.
Hensel,K. [04]: Neue Begründung der Arithmetik, J. Reine Angew. Math., **127**, 1904, 51–84.
Hensel,K. [05a]: Über eine neue Begründung der Theorie der algebraischen Zahlen, J. Reine Angew. Math., **128**, 1905, 1–32.
Hensel,K. [05b]: Über die zu einem algebraischem Körper gehörigen Invarianten, J. Reine Angew. Math., **129**, 1905, 68–85
Hensel,K. [07]: Über die arithmetische Eigenschaften der Zahlen, Jahresber. Deutsch. Math.-Verein., **16**, 1907, 299–313, 386–393, 473–496.

Hensel,K. [08]: *Theorie der algebraischen Zahlen*, Leipzig-Berlin 1908.

Hensel,K. [09]: Über die zu einer algebraischer Gleichung gehörigen Auflösungskörper, J. Reine Angew. Math., **136**, 183–209.

Hensel,K. [13]: *Zahlentheorie*, Berlin-Leipzig 1913.

Hensel,K. [14a]: Über die Grundlagen einer neuen Theorie der quadratischeer Zahlkörper, J. Reine Angew. Math., **144**, 1914, 57–70.

Hensel,K. [14b]: Die Exponentialdarstellung der Zahlen eines algebraischen Zahlkörpers für den Bereich eines Primdivisors, Festschrift H. A. Schwarz, Berlin 1914.

Hensel,K. [15]: Untersuchungen der Zahlen eines algebraischen Körpers für den Bereich eines beliebigen Primteilers, J. Reine Angew. Math., **145**, 1915, 92–113.

Hensel,K. [16a]: Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers, J. Reine Angew. Math., **146**, 1916, 189–215.

Hensel,K. [16b]: Untersuchung der Zahlen eines algebraischen Körpers für eine beliebige Primteilerpotenz als Modul, J. Reine Angew. Math., **146**, 1916, 216–228.

Hensel,K. [17]: Allgemeine Theorie der Kongruenzklassgruppen und ihrer Invarianten in algebraischen Körpern, J. Reine Angew. Math., **147**, 1917, 1–15.

Hensel,K. [18]: Eine neue Theorie der algebraischen Zahlen, Math. Z., **2**, 1918, 433–452.

Hensel,K. [21a]: Über die Zerlegung der Primteiler in relativ cyklischen Körpern, nebst einer Anwendung auf die Kummerschen Körper, J. Reine Angew. Math., **151**, 1921, 112–120.

Hensel,K. [21b]: Über die Zerlegung der Primteiler eines beliebigen Zahlkörpers in einem auflösbaren Oberkörper, J. Reine Angew. Math., **151**, 1921, 200–209.

Hensel,K. [21c]: Zur multiplikativen Darstellung der algebraischen Zahlen für den Bereich eines Primteilers, J. Reine Angew. Math., **151**, 1921, 210–212.

Hensel,K. [27]: Die Exponentialdarstellung der rationalen Zahlen für den Bereich einer Primzahl, S.-B. Marburg, **62**, 1927, 431–434.

Hensley,D. [76]: An asymptotic inequality concerning primes in contours for the case of quadratic number fields, Acta Arith., **28**, 1975/76, 69–79.

Herbrand,J. [30a]: Détermination des groupes de ramification d'un corps a partir de ceux d'un sur-corps, C.R. Acad. Sci. Paris, **191**, 1930, 980–982.

Herbrand,J. [30b]: Nouvelle démonstration et généralisation d'un théorème de Minkowski, C.R. Acad. Sci. Paris, **191**, 1930, 1282–1285.

Herbrand,J. [31a]: Sur la théorie des groupes de décomposition, d'inertie et de ramification, J. math. pures appl., (9) **10**, 1931, 481–498.

Herbrand,J. [31b]: Sur les unités d'un corps algébrique, C.R. Acad. Sci. Paris, **192**, 24–27; corr. p.188.

Herbrand,J. [31c]: Sur la théorie des corps des nombres de degré infini, C.R. Acad. Sci. Paris, **193**, 1931, 504–506.

Herbrand,J. [32a]: Sur les classes des corps circulaires, J. math. pures appl., (9) **11**, 1932, 417–441.

Herbrand,J. [32b]: Théorie arithmétique des corps des nombres de degré infini, Math. Ann., **106**, 1932, 473–501; II, **108**, 1933, 699–717.

Herbrand,J. [32c]: Sur les théorèmes du genre principal et des idéaux principaux, Abh. Math. Sem. Univ. Hamburg, **9**, 1932, 84–92.

Herbrand,J. [32d]: Une propriété de discriminant des corps algébriques, Ann. Sci. École Norm. Sup., (3) **49**, 1932, 105–112.

Herglotz,G. [23]: Über die Kroneckersche Grenzformel für reelle, quadratische Körper, Ber. Verh. Sächs. Akad. Wiss. Leipzig, **75**, 1923, 3–14; II, 31–37.

Hermite,C. [50]: Sur different objects de la théorie des nombres (Lettres de M.Hermite à M.Jacobi), J. Reine Angew. Math., **40**, 1850, 261–278, 279–315 = *Oeuvres*, **I**, 100–163, Paris 1905.

Hermite,C. [57]: Extrait d'une lettre de M.C.Hermite à M.Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés, J. Reine Angew. Math., **53**, 1857, 182–192 = *Oeuvres*, **I**, 414–428, Paris 1905.

Herz,C.S. [66]: Construction of class fields, in: *Seminar on Complex Multiplication*, Lecture Notes in Math., **21**, Springer 1966.

Heß,F.,Pauli,S.,Pohst,M.E. [03]: Computing the multiplicative group of residue class rings, Math. Comp., **72**, 2003, 1531–1548.

Hewitt,E.,Ross,K. [63]: *Abstract Harmonic Analysis*, Springer 1963.

Hida,H. [78]: On the values of Hecke's L-functions at non-positive integers, J. Math. Soc. Japan, **30**, 1978, 249–278.

Higman,G. [40]: The units of group rings, Proc. London Math. Soc., (2) **46**, 1940, 231–248.

Hijikata,H. [63]: Hasse's principle on quaternionic anti-hermitian forms, J. Math. Soc. Japan, **15**, 1963, 165–175.

Hilano,T. [74]: On the zeros of Hecke's L-functions, Sci. Papers College Gen. Ed. Univ. Tokyo, **24**, 1974, 9–24.

Hilbert,D. [90]: Ueber die Theorie der algebraischen Formen, Math. Ann., **36**, 1890, 473–534 = *Gesammelte Abhandlungen*, **II**, 199–257, Chelsea 1965.

Hilbert,D. [94a]: Grundzüge einer Theorie des Galoisschen Zahlkörpers, Nachr. Ges. Wiss. Göttingen, 1894, 224–236 = *Gesammelte Abhandlungen*, **I**, 13–23, Chelsea 1965.

Hilbert,D. [94b]: Über die Zerlegung der Ideale eines Zahlkörpers in Primideale, Math. Ann., **44**, 1894, 1–8 = *Gesammelte Abhandlungen*, **I**, 6–12, Chelsea 1965.

Hilbert,D. [96]: Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1896, 29–39 = *Gesammelte Abhandlungen*, **I**, 53–62, Chelsea 1965.

Hilbert,D. [97]: Die Theorie der algebraischen Zahlkörper, Jahresber. Deutsch. Math.-Verein., **4**, 1897, 175–546 = *Gesammelte Abhandlungen*, **I**, 63–363, Chelsea 1965. [English translation: *The Theory of Algebraic Number Fields*, Springer 1998.]

Hilbert,D. [99]: Über die Theorie des relativquadratischen Zahlkörpers, Math. Ann., **51**, 1899, 1–127.

Hinz,J. [76]: Über Nullstellen der Heckeschen Zetafunktionen in algebraischen Zahlkörpern, Acta Arith., **31**, 1976, 167–193.

Hinz,J. [77]: Über Nullstellen der m-ten Ableitung der Dedekindschen Zetafunktion, J. Number Theory, **9**, 1977, 535–560.

Hinz,J. [79]: A mean value theorem for the Dedekind zeta function of a quadratic number field, Monatsh. Math., **87**, 1979, 229–239.

Hinz,J. [80]: Eine Erweiterung des nullstellenfreies Bereiches der Heckeschen Zetafunktion und Primideale in Idealklassen, Acta Arith., **38**, 1980/81, 209–254.

Hinz,J. [81]: On the theorem of Barban-Davenport-Halberstam in algebraic number fields, J. Number Theory, **13**, 1981, 463–484.

Hinz,J. [82]: Eine Anwendung der Selbergschen Siebmethode in algebraischen Zahlkörpern, Acta Arith., **41**, 1982, 223–254.

Hinz,J. [83a]: Character sums in algebraic number fields, J. Number Theory, **17**, 1983, 52–70.

Hinz,J. [83b]: Character sums and primitive roots in algebraic number fields, Monatsh. Math., **95**, 1983, 275–286.

Hinz,J. [83c]: The average order of magnitude of least primitive roots in algebraic number fields, Mathematika, **30**, 1983, 11–25.
Hinz,J. [84]: Some applications of sieve methods in algebraic number fields, Manuscripta Math., **48**, 1984, 117–137.
Hinz,J. [86]: A note on Artin's conjecture in algebraic number fields, J. Number Theory, **22**, 1986, 334–349.
Hinz,J. [87]: Methoden des grossen Siebes in algebraischen Zahlkörpern, Manuscripta Math., **57**, 1987, 181–194.
Hinz,J.G. [88]: A generalization of Bombieri's prime number theorem to algebraic number fields, Acta Arith., **51**, 1988, 173–193.
Hinz,J. [93]: On the prime ideal theorem, J. Indian Math. Soc., (N.S.) **59**, 1993, 243–260,
Hinz,J. [96]: A note on Bombieri-type result in algebraic prime number theory, Archiv Math., **67**, 1996, 16–22.
Hinz,J. [03]: An application of algebraic sieve theory, Archiv Math., **80**, 2003, 586–599.
Hinz,J.,Lodemann,M. [94]: On Siegel zeros of Hecke-Landau zeta-functions, Monatsh. Math., **118**, 1994, 231–248.
Hirabayashi,M. [98]: A generalization of Maillet and Demyanenko determinants, Acta Arith., **83**, 1998, 391–397.
Hirabayashi,M. [99]: A relative class number formula for an imaginary abelian field by means of Demjanenko matrix, in: *Proceedings of the Conference on Analytic and Elementary Number Theory (Vienna 1996)*, 81–91, Wien 1999.
Hiramatsu,T. [82]: Higher reciprocity laws and modular forms of weight one, Comment. Math. Univ. St. Paul, **31**, 1982, 75–85.
Hirzebruch,F. [73]: The Hilbert modular group and some algebraic surfaces, Trudy Mat. Inst. Steklov., **132**, 1973, 55–66.
Hirzebruch,F. [76]: Hilbert modular surfaces and class numbers, Astérisque, **32/33**, 1976, 151–164.
Hochschild,H.,Nakayama,T. [52]: Cohomology in class field theory, Ann. of Math., (2) **55**, 1952, 248–366.
Hodges,W. [74]: Six impossible rings, J. Algebra, **31**, 1974, 218–244.
Hoffstein,J. [79]: Some analytic bounds for zeta functions and class numbers, Invent. math., **55**, 1979, 37–47.
Hoffstein,J. [80]: On the Siegel-Tatuzawa theorem, Acta Arith., **38**, 1980, 167–174.
Hofreiter,N. [35]: Quadratische Körper mit und ohne Euklidischen Algorithmus, Monatsh. Math. Phys., **42**, 1935, 397–400.
Holland,D. [92]: Additive Galois module structure and Chinburg's invariant, J. Reine Angew. Math., **425**, 1992, 193–218.
Holland,D. [94]: Chinburg's third invarianr in the factorisability defect class group, Canad. J. Math., **46**, 1994, 324–342.
Holland,D.,Wilson,S.M.J. [93]: Fröhlich's and Chinburg's conjectures in the factorisability defect of the class group, J. Reine Angew. Math., **442**, 1993, 1–17.
Holland,D.,Wilson,S.M.J. [94]: Factor equivalence of rings of integers and Chinburg's invariant in the defect class group, J. London Math. Soc., (2) **49**, 1994, 417–441.
Holzer,L. [50]: Zur Klassenzahl in reinen Zahlkörpern von ungeraden Primzahlgrad, Acta Math., **83**, 1950, 327–348.
Honda,T. [60a]: On absolute class fields of certain algebraic number fields, J. Reine Angew. Math., **203**, 1960, 80–89.
Honda,T. [60b]: On the absolute ideal class group of relatively metacyclic number fields of a certain type, Nagoya Math. J., **17**, 1960, 171–179.

Honda,T. [68]: On real quadratic fields whose class numbers are multiples of 3, J. Reine Angew. Math., **233**, 1968, 101–102.
Honda,T. [71]: Pure cubic fields whose class numbers are multiples of three, J. Number Theory, **3**, 1971, 7–12.
Honda,T. [75]: A few remarks on class numbers of imaginary quadratic number fields, Osaka Math. J., **12**, 1975, 19–21.
Hooley,C. [84]: On the Pellian equation and the class number of indefinite binary quadratic forms, J. Reine Angew. Math., **353**, 1984, 98–131.
Hooper,J.,Snaith,V.,van Tran,N. [00]: The second Chinburg conjecture for quaternion fields, Mem. Amer. Math. Soc., **148**, 2000, 1–133.
Horie,K. [89]: On the class number of cyclotomic fields, Manuscripta Math., **65**, 1989, 465–477.
Horie,K. [90]: Multiplicative groups in some infinite algebraic number fields, Archiv Math., **54**, 1990, 32–35.
Horie,K. [92]: On the ratio between relative class numbers, Math. Z., **211**, 1992, 505–521.
Horie,K. [93b]: On the exponents of ideal class groups of cyclotomic fields, Proc. Amer. Math. Soc., **119**, 1993, 1049–1052.
Horie,K.,Horie,M. [90a]: On the exponents of ideal class groups of CM-fields, in: *Analytic Number Theory, (Tokyo 1988)*, Lecture Notes in Math., **1434**, 143–148, Springer 1990.
Horie,K.,Horie,M. [90b]: CM-fields and exponents of their ideal class groups, Acta Arith., **55**, 1990, 157–170.
Horie,K.,Ogura,H. [95]: On the ideal class groups of imaginary abelian fields with small conductor, Trans. Amer. Math. Soc., **347**, 1995, 2517–2532.
Horie,M. [83]: On the genus field in algebraic number fields, Tokyo J. Math., **6**, 1983, 363–380.
Horie,M. [91]: The Hasse principle for elementary abelian fields, Mem. Fac. Sci. Kyushu Univ., **45**, 1991, 41–54.
Horie,M. [93]: The Hasse norm principle for elementary abelian extensions, Proc. Amer. Math. Soc., **118**, 1993, 47–56.
Hua,L.K. [42]: On the least solution of Pell's equation, Bull. Amer. Math. Soc., **48**, 1942, 731–735.
Huard,J.G.,Spearman,B.K., Williams,K.S. [94]: A short proof of the formula for the conductor of an abelian cubic field, Det Kong. Norske Vidensk. Selsk., 1994, No.2.
Huard,J.G.,Spearman,B.K., Williams,K.S. [95]: Integral bases for quartic fields with quadratic subfields, J. Number Theory, **51**, 1995, 87–102.
Huckaba,J.A.,Papick,I.J. [81]: A localization of $R[X]$, Canad. J. Math., **33**, 1981, 103–115.
Hudson,R.H.,Williams,K.S. [82]: Class number formulae of Dirichlet type, Math. Comp., **39**, 725–732.
Hudson,R.H.,Williams,K.S. [90]: The integers of a cyclic quartic field, Rocky Mountain J. Math., **20**, 1990, 145–150.
Hughes,J.,Mollin,R. [83]: Totally positive units and squares, Proc. Amer. Math. Soc., **87**, 1983, 613–616.
Humbert,P. [40]: Sur les nombres de classes de certains corps quadratiques, Comment. Math. Helv., **12**, 1939/40, 233–245; add.: **13**, 1940/41, p.67.
Hunter,J. [56]: A generalization of the inequality of the arithmetic-geometric mean, Proc. Glasgow Math. Assoc., **2**, 1956, 149–158.
Hunter,J. [57]: The minimum discriminant of quintic fields, Proc. Glasgow Math. Assoc., **3**, 1957, 57–67.

Hürlimann,W.,Saltman,D. [85]: On the exponent of the norm residue group, Proc. Amer. Math. Soc., **93**, 1985, 417–419.

Hurrelbrink,J. [94]: Circulant graphs and 4-ranks of ideal class groups, Canad. J. Math., **46**, 1994, 169–183.

Hurwitz,A. [82]: Einige Eigenschaften der Dirichlet'schen Functionen

$$F(s) = \sum \left(\frac{D}{n}\right) \cdot \frac{1}{n^s},$$

die bei der Bestimmung der Classenanzahlen binärer quadratischer Formen auftreten. Zeitschr. Math. Phys., **27**, 86–101=*Mathematische Werke*, **I**, 72—88, Birkhäuser 1932.

Hurwitz,A. [94]: Über die Theorie de Ideale, Nachr. Ges. Wiss. Göttingen, 1894, 291–298 = *Mathematische Werke*, **II**, 191–197, Birkhäuser 1932.

Hurwitz,A. [95a]: Über einen Fundamentalsatz der arithmetischer Theorie der algebraischen Grössen, Nachr. Ges. Wiss. Göttingen, 1895, 230–240 = *Mathematische Werke*, **II**, 198–207, Birkhäuser 1932.

Hurwitz,A. [95b]: Die unimodularen Substitutionen in einem algebraischen Zahlenkörper, Nachr. Ges. Wiss. Göttingen, 1895, 244–268 = *Mathematische Werke*, **II**, 244–268, Birkhäuser 1932.

Hurwitz,A. [95c]: Zur Theorie der algebraischen Zahlen, Nachr. Ges. Wiss. Göttingen, 1895, 324–331 = *Mathematische Werke*, **II**, 236–243, Birkhäuser 1932.

Hurwitz,A. [95d]: Über die Anzahl der Classen binärer quadratischer Formen von negativer Determinante, Acta Math., **19**, 1895, 389–397 = *Mathematische Werke*, **II**, 208–235, Birkhäuser 1932.

Hurwitz,A. [99]: Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, Math. Ann., **51**, 1899, 196–226 = *Mathematische Werke*, **II**, 342–373, Birkhäuser 1932.

Hurwitz,A. [26]: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Math. Z., **25**, 1926, 661–665 = *Mathematische Werke*, **II**, 733–736, Birkhäuser 1932.

Hutchinson,K. [95a]: Norm groups of global fields, J. Number Theory, **50**, 1995, 323–328.

Hutchinson,K. [95b]: On relative integral bases for unramified extensions, Acta Arith., **70**, 1995, 279–286.

Huxley,M.N. [68]: The large sieve inequality for algebraic number fields, Mathematika, **15**, 1968, 178–187; II, Proc. London Math. Soc., (3) **21**, 1970, 108–128; III, J. London Math. Soc., (2) **3**, 1971, 233–240.

Huxley,M.N. [00]: The number of ideals in a quadratic field, II, Israel J. Math., **120**, 2000, 125–153.

Huxley,M.N.,Watt,N. [94]: The number of ideals in a quadratic field, Proc. Indian Acad. Sci., **104**, 1994, 157–165.

Hyyrö,S. [67]: Über eine Determinantenidentität und den ersten Faktor der Klassenzahl des Kreiskörpers, Ann. Acad. Sci. Fenn. Ser. A1, **398**, 1967, 1–7.

Hymo,J.A.,Parry,C.J. [90]: On relative integral bases for cyclic quartic fields, J. Number Theory, **34**, 1990, 189–197.

Hymo,J.A.,Parry,C.J. [92]: On relative integral bases for pure quartic fields, Indian J. Pure Appl. Math., **23**, 1992, 359–376.

Ichimura,H. [82]: On 2-rank of the ideal class groups of totally real number fields, Proc. Japan Acad. Sci., **58**, 1982, 329–332.

Ichimura,H. [95]: On p-adic L-functions and normal bases of rings of integers, J. Reine Angew. Math., **462**, 1995, 169–184.

Ichimura,H. [96]: On a normal integral bases problem over cyclotomic Z_p-extensions, J. Math. Soc. Japan, **48**, 1996, 689–703.
Ichimura,H. [00a]: On a power integral bases problem in cyclotomic Z_p-extensions, J. Algebra, **234**, 2000, 90–100.
Ichimura,H. [00b]: A note on integral bases of unramified cyclic extensions of prime degree, Abh. Math. Sem. Univ. Hamburg, **70**, 2000, 275–279.
Ichimura,H. [01a]: On power integral bases of unramified cyclic extensions of prime degree, J. Algebra, **235**, 2001, 104–112.
Ichimura,H. [01b]: Note on the ring of integers of a Kummer extension of prime degree, II,III,IV, Proc. Japan Acad. Sci., **77**, 2001, 25–28, 71–73, 92–94.
Ichimura,H.,Kawamoto,F. [03]: An infinite family of totally real fields, Acta Arith., **106**, 2003, 171–181.
Ichimura,H.,Sumida,H. [97]: On the Iwasawa invariants of certain real Abelian fields, Tôhoku Math. J., (2) **49**, 1997, 203–215; II, Internat. J. Math., **7**, 1996, 721–744.
Ichimura,H.,Sumida,H. [00]: A note on integral bases of unramified cyclic extensions of prime degree, II, Manuscripta Math., **104**, 2001, 201–210.
Idelhadj,A.,Yahya,A. [00]: Socle-fine characterization of Dedekind domains and regular rings, in *Algebra and Number Theory (Fez)*, 157–163, Marcel Dekker, 2000.
Iimura,K. [71]: A criterion for the class number of a pure quintic field to be divisible by 5, J. Reine Angew. Math., **292**, 1971, 201–210.
Iimura,K. [79a]: Dihedral extensions of Q of degree $2l$ which contain non-Galois extensions with class number not divisible by l, Acta Arith., **35**, 1979, 385–394.
Iimura,K. [79b]: On 3-class groups of non-Galois cubic fields, Acta Arith., **35**, 1979, 395–402.
Iimura,K. [80]: On the unit group of certain sextic number fields, Abh. Math. Sem. Univ. Hamburg, **50**, 1980, 32–39.
Iimura,K. [81a]: On the l-class group of an algebraic number field, J. Reine Angew. Math., **322**, 1981, 136–144.
Iimura,K. [81b]: A note on the Stickelberger ideal of conductor level, Archiv Math., **36**, 1981, 45–52.
Ikeda,M. [75a]: On the group automorphisms of the absolute Galois group of the rational number field, Archiv Math., **26**, 1975, 250–252.
Ikeda,M. [75b]: Completeness of the absolute Galois group of the rational number field, Archiv Math., **26**, 1975, 602–605.
Ikeda,M. [77]: Completeness of the absolute Galois group of the rational number field, J. Reine Angew. Math., **291**, 1977, 1–22.
Inaba,E. [35]: Über Klassenzahlen abelscher Zahlkörper, Proc. Imper. Acad. Japan, **11**, 1935, 81–82.
Inaba,E. [37]: Über die absoluten Idealklassengruppen algebraischer Zahlkörper, Japan J. Math., **13**, 1937, 81–84.
Inaba,E. [40]: Über die Struktur der l-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad l, J. Fac. Sci. Univ. Tokyo, **4**, 1940, 61–115.
Inaba,E. [41]: Klassenkörpertheoretische Deutung der Struktur der Klassengruppe des zyklischen Zahlkörpers, Proc. Imp. Acad. Japan, **17**, 1941, 125–128.
Inaba,E. [52]: Note on relative complete fields, Natur. Sci. Rep. Ochanomizu Univ., **3**, 1952, 5–9.
Indlekofer,K.H.,Kátai,I.,Racskó,P. [92]: Number systems and fractal geometry, in: *Probability Theory and Applications*, 319–334. Kluwer 1992.
Inkeri,K. [55]: Über die Klassenzahl des Kreiskörpers der l-ten Einheitswurzeln, Ann. Acad. Sci. Fenn. Ser. A1, **199**, 1955, 1-12.
Ireland,K.F.,Rosen,M.I. [82]: *A Classical Introduction to Modern Number Theory*, Springer 1982; 2nd ed. 1990.

Iseki,K. [53]: On a general divisor problem in algebraic number fields, Natur. Sci. Rep. Ochanomizu Univ., **4**, 1953, 1–21.
Ishibashi,M. [93]: A sufficient arithmetical condition for the ideal class group of an imaginary quadratic field to be cyclic, Proc. Amer. Math. Soc., **117**, 1993, 613–618.
Ishida,M. [57]: On the divisibility of Dedekind's zeta-functions, Proc. Japan Acad. Sci., **33**, 1957, 293–297.
Ishida,M. [69]: A note on class numbers of algebraic number fields, J. Number Theory, **1**, 1969, 65–69.
Ishida,M. [70]: Class numbers of algebraic number fields of Eisensteinian type, J. Number Theory, **2**, 1970, 404–413; II, **6**, 1974, 99–104.
Ishida,M. [71]: On algebraic number fields with even class-numbers, J. Reine Angew. Math., **247**, 1971, 118–122.
Ishida,M. [73]: Fundamental units of certain algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **39**, 1973, 245–250.
Ishida,M. [74]: Some unramified abelian extensions of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **39**, 1973, 245–250.
Ishida,M. [75]: On the 2-rank of the ideal class group of algebraic number fields, J. Reine Angew. Math., **273**, 1975, 165–169.
Ishida,M. [76]: *The Genus Field of Algebraic Number Fields*, Lecture Notes in Math., **555**, Springer 1976.
Ishikawa,M.,Kitaoka,Y. [98]: On the distribution of units modulo prime ideals in real quadratic fields, J. Reine Angew. Math., **494**, 1998, 65–72.
Iskovskikh,V.A. [71]: A counterexample to the Hasse principle for a system of two quadratic forms in five variables, Mat. Zametki, **10**, 1971, 253–257. (Russian)
Ito,H. [77]: A note on the law of decomposition of primes in certain Galois extensions, Proc. Japan Acad. Sci., **53**, 1977, 115–118.
Ito,H. [89]: On a product related to the cubic Gauss sum, J. Reine Angew. Math., **395**, 1989, 202–213.
Itoh,T. [98]: A construction of normal bases over the Hilbert p-class field of imaginary quadratic fields, Proc. Japan Acad. Sci., **74**, 1998, 25–28.
Iwasaki,K. [52]: Simple proof of a theorem of Ankeny on Dirichlet series, Proc. Japan Acad. Sci., **28**, 1952, 555–557.
Iwasawa,K. [53a]: On the ring of valuation vectors, Ann. of Math., (2) **57**, 1953, 331–356.
Iwasawa,K. [53b]: On solvable extensions of algebraic number fields, Ann. of Math., (2) **58**, 1953, 548–572.
Iwasawa,K. [53c]: A note on Kummer extensions, J. Math. Soc. Japan, **5**, 1953, 253–262.
Iwasawa,K. [55a]: A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20**, 1955, 257–258.
Iwasawa,K. [55b]: On Galois groups of local fields, Trans. Amer. Math. Soc., **80**, 1955, 448–469.
Iwasawa,K. [58]: On some invariants of cyclotomic fields, Amer. J. Math., **80**, 1958, 773–783; corr., **81**, 1959, p.280.
Iwasawa,K. [59a]: On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., **65**, 1959, 183–226.
Iwasawa,K. [59b]: Sheaves for algebraic number fields, Ann. of Math., (2) **69**, 1959, 183–226.
Iwasawa,K. [59c]: On some properties of Γ-finite modules, Ann. of Math., (2) **70**, 1959, 291–312.
Iwasawa,K. [59d]: On the theory of cyclotomic fields, Proc. Symposia Pure Math., **8**, 1959, 530–561.

Iwasawa,K. [60]: On local cyclotomic fields, J. Math. Soc. Japan, **12**, 1960, 16–21.
Iwasawa,K. [62]: A class number formula for cyclotomic fields, Ann. of Math., (2) **76**, 1962, 171–179.
Iwasawa,K. [65]: Some modules in the theory of cyclotomic fields, Proc. Symposia Pure Math., **8**, 1965, 66–69.
Iwasawa,K. [66]: A note on ideal class group, Nagoya Math. J., **27**, 1966, 239–247.
Iwasawa,K. [72a]: *Lectures on p-adic L-functions*, Princeton 1972.
Iwasawa,K. [72b]: On the μ-invariants of cyclotomic fields, Acta Arith., **21**, 1972, 99–101.
Iwasawa,K. [73a]: On Z_l-extensions of algebraic number fields, Ann. of Math., (2) **98**, 1973, 248–326.
Iwasawa,K. [73b]: On the μ-invariants of Z_l-extensions, in: *Number Theory, Algebraic Geometry and Commutative Algebra*, 1–11, Tokyo 1973.
Iwasawa,K. [75]: A note on Jacobi sums, Symposia Math., **15**, 1975, 447–459.
Iwasawa,K. [76]: A note on cyclotomic fields, Invent. math., **36**, 1976, 115–123.
Iwasawa,K. [80]: *Local Class Field Theory*, Iwanami Shoten 1980. (Japanese) [Russian translation: Moskva 1983.]
Iwasawa,K. [86]: *Local Class Field Theory*, Oxford University Press 1986.
Iwasawa,K. [89]: A note on capitulation problem for number fields, Proc. Japan Acad. Sci., **65**, 1989, 59–61; II, 183–186.
Iwasawa,K. [92]: Letter to J.Dieudonné, in: *Zeta Functions in Geometry (Tokyo 1990)*, 445–450. Tokyo 1992.
Iwata,H. [72]: Algebraic number fields embedded in Q_p, Bull. Fac. Sci. Ibaraki Univ., A, **4**, 1972, 21–28.
Iyanaga,S. [31]: Über den allgemeinen Hauptidealsatz, Japan J. Math., **7**, 1931, 315–333.
Iyanaga,S. [34]: Zum Beweis des Hauptidealsatzes, Abh. Math. Sem. Univ. Hamburg, **10**, 1934, 349–357.
Iyanaga,S. [39]: Über die allgemeinen Hauptidealformeln, Monatsh. Math. Phys.. **48**, 1939, 400–407.
Iyanaga,S. [75]: *The Theory of Numbers*, North-Holland 1975.
Iyanaga,S.,Tamagawa,T. [51]: Sur la théorie du corps de classes sur le corps des nombres rationnels, J. Math. Soc. Japan, **3**, 1951, 220–227.
Jacobi,C.G.J. [32]: Observatio arithmetica de numero classium divisorum quadraticorum formae $aa + Azz$, designante a numerum primum formae $4n + 3$, J. Reine Angew. Math., **9**, 1832, 189–192.
Jacobi,C.G.J. [39]: Ueber die complexen Primzahlen, welche in der Theorie der 5-ten, 8-ten und 12-ten Potenzen zu betrachten sind, J. Reine Angew. Math., **19**, 1839, 314–318.
Jacobi,C.G.J. [46]: Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie, J. Reine Angew. Math., **30**, 1846, 166–182.
Jacobi,C.G.J. [68]: Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus drei vorhergehenden gebildet wird, J. Reine Angew. Math., **69**, 1868, 29–64.
Jacobinski,H. [63]: Über die Hauptordnung eines Körpers als Gruppenmodul, J. Reine Angew. Math., **213**, 1963, 151–164.
Jacobson,B. [64]: Sums of distinct divisors and sums of distinct units, Proc. Amer. Math. Soc., **15**, 1964, 179–183.
Jacobson,E.,Vélez,W.Y. [85]: On the adèle rings of radical extensions of the rationals, Archiv Math., **45**, 1985, 12–20.
Jacobson,E.,Vélez,W.Y. [90]: Fields arithmetically equivalent to a radical extensions of the rationals, J. Number Theory, **35**, 1990, 227–246.

Jacobson,M.J.Jr.,Lukes,R.F.,Williams,H.C. [95]: An investigation of bounds for the regulator of quadratic fields, Exposition Math., **4**, 1995, 211–225.
Jacobsthal,E. [13]: Diophantische Gleichungen im Bereich aller ganzen algebraischen Zahlen, Math. Ann., **74**, 1913, 31–65.
Jakubec,S. [93]: On divisibility of class number of real abelian fields of prime conductor, Abh. Math. Sem. Univ. Hamburg, **63**, 1993, 67–86.
Jakubec,S. [94a]: On Vandiver's conjecture, Abh. Math. Sem. Univ. Hamburg, **64**, 1994, 105–124.
Jakubec,S. [94b]: On the divisibility of h^+ by the prime 3, Rocky Mountain J. Math., **24**, 1994, 1467–1473.
Jakubec,S. [94c]: On the divisibility of h^+ by the prime 5, Math. Slovaca, **44**, 1994, 651–661.
Jakubec,S. [95]: Connection between Wieferich congruence and divisibility of h^+, Acta Arith., **71**, 1995, 55–64.
Jakubec,S. [96a]: Connection between congruences $n^{q-1} \equiv 1 \pmod{q^2}$ and divisibility of h^+, Abh. Math. Sem. Univ. Hamburg, **66**, 1996, 151–158.
Jakubec,S. [96b]: Congruence of Ankeny-Artin-Chowla type for cyclic fields of prime degree l, Math. Proc. Cambridge Philos. Soc., **119**, 1996, 17–22.
Jakubec,S. [97]: On divisibility of the class number h^+ of the real cyclotomic fields $Q(\zeta_p + \zeta_p^{-1})$ by primes $q \leq 5000$, Abh. Math. Sem. Univ. Hamburg, **67**, 1997, 269–280.
Jakubec,S. [98]: On divisibility of the class number h^+ of the real cyclotomic fields of prime degree l, Math. Comp., **67**, 1998, 369–398.
Jakubec,S.,Kostra,J. [92]: A note on normal bases of ideals, Math. Slovaca, **42**, 1992, 677–684.
Jakubec,S.,Kostra,J. [98]: On the existence of a normal basis for an ambiguous ideal, Atti Sem. Mat. Fiz. Univ. Modena, **46**, 1998, 125–129.
Janssen,U. [82]: Über Galoisgruppen lokaler Körper, Invent. math., **70**, 1982/83, 53–69.
Janssen,U.,Wingberg,K. [82]: Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper, Invent. math., **70**, 1982/83, 71–98.
Janusz,G. [73]: *Algebraic Number Fields*, Academic Press 1973; 2nd ed. Amer. Math. Soc. 1996.
Járási,I. [02]: Computing all elements of given index in sextic fields with a cubic subfield, Acta Math. Inf. Univ. Ostraviensis, **10**, 2002, 49–59.
Járási,I. [03]: Power integral bases in sextic fields with a cubic subfield, Acta Sci. Math. (Szeged), **69**, 2003, 3–15.
Jarden,M. [74]: On Chebotarev sets, Archiv Math., **25**, 1974, 495–497.
Jarden,M.,Ritter,J. [79]: On the characterization of local fields by their absolute Galois groups, J. Number Theory, **11**, 1979, 1–13.
Jarden,M.,Ritter,J. [80]: Normal automorphisms of absolute Galois groups of $\mathfrak{p}$-adic fields, Duke Math. J., **47**, 1980, 47–56.
Jaulent,J.-F. [79]: *Structures galoisiennes dans les extensions métabeliennes*, Thése, Besançon 1979.
Jaulent,J.-F. [81a]: Remarques sur la structure galoisienne des entiers d'une extension métacyclique de Q, C.R. Acad. Sci. Paris, **293**, 1981, 231–233.
Jaulent,J.-F. [81b]: Sur la l-structure des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels, Publ. Math. Fac. Sci. Besançon, 1979/80 et 1980/81.
Jaulent,J.-F. [81c]: Sur la théorie des genres dans un extension cyclique de degré l^m d'un corps de nombres métabelienne sur un sous-corps, Publ. Math. Fac. Sci. Besançon, 1979/80 et 1980/81.

Jaulent,J.-F. [81d]: Unités et classes dans les extensions métabéliennes du degré nl^s sur un corps de nombres algébriques, Ann. Inst. Fourier, **31**, 1981, no.1, 39–62.
Jaulent,J.-F. [82]: Sur la théorie des genres dans les tours métabéliennes, Sém. Théor. Nombres Bordeaux, 1981/82, exp, 24.
Jaulent,J.-F. [88]: L'état actuel du problème de la capitulation, Sém. Théor. Nombres Bordeaux, 1987/88, exp. 17.
Jehne,W. [54]: Zur moderner Klassenkörpertheorie, S.Ber. Deutsch. Akad. Wiss., 1954, no.3, 1–8.
Jehne,W. [59]: Bemerkung über die p-Klassengruppe des p-ten Kreiskörpers, Archiv Math., **10**, 1959, 422–427.
Jehne,W. [77a]: Über die Einheiten- und Divisorenklassengruppe von reellen Frobeniuskörpern von Maximaltyp, Math. Z., **152**, 1977, 223–252.
Jehne,W. [77b]: Kronecker classes of algebraic number fields, J. Number Theory, **9**, 1977, 279–320.
Jehne,W. [77c]: On Kronecker classes of atomic extensions, Proc. London Math. Soc., (3) **34**, 1977, 32–64.
Jehne,W. [79]: On knots in algebraic number theory, J. Reine Angew. Math., **311/312**, 1979, 215–254.
Jehne,W. [82]: Der Hassesche Normensatz und seine Entwicklung, Mitt. Math. Ges. Hamburg, **11**, 1982, 143–153.
Jenkner,W. [92]: Les corps p-adiques dont les groupes de Galois absolus sont isomorphes, Astérisque, **1992**, 221–226.
Jensen,C.U. [60]: Über die Führer einer Klasse Heckescher Grössencharaktere, Math. Scand., **8**, 1960, 81–96.
Jensen,C.U. [62]: On the solvability of a certain class of non-Pellian equations, Math. Scand., **10**, 1962, 71–84.
Jensen,C.U. [63]: On characterizations of Prüfer rings, Math. Scand., **13**, 1963, 90–98.
Jensen,C.U. [64]: A remark on relative integral bases for infinite extensions of finite number fields, Mathematika, **11**, 1964, 64–66.
Jensen,K.L. [15]: Numbertheoretical properties of Bernoulli numbers, Nyt Tidsskr. Mat., **26**, 1915, B, 73–83. (Danish)
Jha,V. [95]: Faster computation of the first factor of the class number of $Q(\zeta_p)$, Math. Comp., **64**, 1995, 1705–1710.
Ji,C. [98]: On normal integral bases, Northeast. Math. J., **14**, 1998, 105–111.
Johnson,D. [79]: Mean values of Hecke L-functions, J. Reine Angew. Math., **305**, 1979, 195–209.
Johnson,D.H.,Queen,C.S.,Sevilla,A.N. [85]: Euclidean real quadratic number fields, Archiv Math., **44**, 1985, 340–347.
Jones,B.W. [49]: The composition of binary quadratic forms, Amer. Math. Monthly, **56**, 1949, 380–391.
Jones,J.W.,Roberts,D.P. [99]: Sextic number fields with discriminant $(-1)^j 2^a 3^b$, in: *Number Theory (Ottawa, ON, 1996)*, 141–172. Amer. Math. Soc. 1999.
Jones,J.W.,Roberts,D.P. [03]: Septic fields with discriminant $\pm 2^a 3^b$, Math. Comp., **72**, 2003, 1975–1985.
Jordan,J.H. [67]: Character sums in $Z(i)/(p)$, Proc. London Math. Soc., (3) **17**, 1967, 1–10.
Jordan,J.H.,Rabung,J.R. [70]: A conjecture of Paul Erdős concerning Gaussian primes, Math. Comp., **24**, 1970, 221–223.
Joris,H. [72]: Ω-Sätze für zwei arithmetische Funktionen, Comment. Math. Helv., **47**, 1972, 220–248.
Jung,S.-W.,Kwon,S,H. [98]: Determination of all imaginary bicyclic biquadratic number fields of class number 3, Bull. Korean Math. Soc., **35**, 1998, 83–89.

Jutila,M. [73]: On character sums and class numbers, J. Number Theory, **5**, 1973, 203–314.

Jutila,M. [77]: Zero-density estimates for L-functions, Acta Arith., **32**, 1977, 55–62.

Kable,A.C. [99]: Power bases in dihedral quartic fields, J. Number Theory, **76**, 1999, 120–129.

Kaczorowski,J. [81a]: A pure arithmetical characterization for certain fields with a given class group, Colloq. Math., **48**, 1981, 327–330.

Kaczorowski,J. [81b]: Completely irreducible numbers in algebraic number fields, Funct. Approx. Comment. Math., **11**, 1981, 95–104.

Kaczorowski,J. [83]: Some remarks on factorization in algebraic number fields, Acta Arith., **43**, 1983, 53–68.

Kaczorowski,J. [84a]: A pure arithmetical definition of the classgroup, Colloq. Math., **48**, 1984, 265–267.

Kaczorowski,J. [84b]: On completely irreducible algebraic integers, in: *Topics in Classical Number Theory (Budapest 1981)*, 831–853, North-Holland 1984.

Kaczorowski,J., Perelli,A. [99a]: On the structure of the Selberg class, I: $0 \leq d \leq 1$, Acta Math., **182**, 1999, 207–241; II: Invariants and conjectures, J. Reine Angew. Math., **524**, 2000, 73–96; III: Sarnak's rigidity conjecture, Duke Math. J., **101**, 2000, 529–554; IV: Basic invariants, Acta Arith., **104**, 2002, 97–116; V: $1 < d < 5/3$, Invent. math., **150**, 2002, 485–516.

Kaczorowski,J., Perelli,A. [99b]: The Selberg class: a survey, in: *Number Theory in Progress*, **II**, 953–992. de Gruyter 1999.

Kaczorowski,J.,Staś,W. [88]: On the number of sign changes in the remainder-term of the prime-ideal theorem, Colloq. Math., **56**, 1988, 185–197.

Kagawa,T. [95]: The Hasse norm principle for the maximal real subfields of cyclotomic fields, Tokyo J. Math., **18**, 1995, 221–229.

Kallies,J.,Snyder,C. [95]: On the values of partial zeta functions of real quadratic fields at nonpositive integers, Math. Nachr., **175**, 1995, 159–191.

Kambayashi,T. [75]: On certain algebraic groups attached to local number fields, J. Reine Angew. Math., **173**, 1975, 41–48.

Kanemitsu,S. [77]: On some bounds for the value of Dirichlet's L-functions $L(s,\chi)$ at the point $s = 1$, Mem. Fac. Sci. Kyushu Univ., A, **31**, 1977, 15–23.

Kanemitsu,S. [78]: A note on the general divisor problem, Mem. Fac. Sci. Kyushu Univ., A, **32**, 1978, 211–221.

Kanemitsu,S.,Kuzumaki,T. [98]: On a generalization of the Maillet determinant, in: *Number Theory (Eger 1966)*, 271–287, de Gruyter 1998; II, Acta Arith., **99**, 2001, 343–361.

Kanno,T. [73]: Automorphisms of the Galois group of the algebraic closure of the rational number field, Kodai Math. Rep., **25**, 1973, 446–448.

Kaplan,P. [72]: Divisibilité par 8 du nombre des classes des corps quadratiques reéls dont le 2-sousgroupe des classes est cyclique, C.R. Acad. Sci. Paris, **275**, 1972, A887–890.

Kaplan,P. [73a]: Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocité quadratique, J. Math. Soc. Japan, **25**, 1973, 596–608.

Kaplan,P. [73b]: 2-groupe des classes et facteurs principaux de $Q(\sqrt{pq})$ ou $p \equiv -q \equiv 1 \pmod 4$, C.R. Acad. Sci. Paris, **276**, 1973, 89–92.

Kaplan,P. [74]: Comparaison des 2-groupes des classes d'idéaux au sense large et au sense étroit d'un corps quadratique réel, Proc. Japan Acad. Sci., **50**, 1974, 688–693.

Kaplan,P. [76]: Sur le 2-groupe des classes d'idéaux des corps quadratiques, J. Reine Angew. Math., **283/284**, 1976, 313–363.

Kaplan,P. [77a]: Unités de norme -1 de $Q(\sqrt{p})$ et corps de classes de degré 8 de $Q(\sqrt{-p})$ oú p est un nombre premier congru à 1 modulo 8, Acta Arith., **32**, 1977, 239–243.

Kaplan,P. [77b]: Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques, Bull. Soc. Math. France, Mém. **49/50**, 113–124.

Kaplan,P. [81]: Nouvelle démonstration d'une congruence modulo 16 entre les nombres de classes d'idéaux de $Q(\sqrt{-2p})$ et $Q(\sqrt{2p})$ pour p premier $\equiv 1 \pmod 4$, Proc. Japan Acad. Sci., **57**, 1981, 507–509.

Kaplan,P.,Williams,K.S. [82a]: On the class numbers of $Q(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1 \pmod 8$, a prime, Acta Arith., **40**, 1982, 289–296.

Kaplan,P.,Williams,K.S. [82b]: Congruences modulo 16 for the class numbers of the quadratic fields $Q(\sqrt{\pm p})$ and $Q(\sqrt{\pm 2p})$ for p a prime congruent to 5 modulo 8, Acta Arith., **40**, 1982, 375–397.

Kaplan,P.,Williams,K.S. [84]: On the strict class number of $Q(\sqrt{2p})$ modulo 16, $p \equiv 1 \pmod 8$ prime, Osaka Math. J., **21**, 1984, 23–29.

Kaplan,P.,Williams,K.S.,Hardy,K. [86]: Divisibilité par 16 des classes au sens strict des corps quadratiques réels dont le deux-groupe des classes est cyclique, Osaka Math. J., **23**, 1986, 479–489.

Kaplansky,I. [47]: Topological methods in valuation theory, Duke Math. J., **14**, 1947, 527–541.

Kaplansky,I. [49]: Elementary divisors and modules, Trans. Amer. Math. Soc., **66**, 1949, 464–491.

Kaplansky,I. [52]: Modules over Dedekind rings and valuation rings, Trans. Amer. Math. Soc., **72**, 1952, 327–340.

Kaplansky,I. [70]: *Commutative Rings*, Allyn & Bacon 1970.

Karatsuba,A.A. [72]: Dirichlet's divisor problem in number fields, Dokl. Akad. Nauk SSSR, **204**, 1972, 540–541. (Russian)

Kátai,I. [94]: Number systems in imaginary quadratic fields, Ann. Univ. Sci. Budapest, Sect. Comput., **14**, 1994, 91–103.

Kátai,I.,Kőrnyei,I. [92]: On number systems in algebraic number fields, Publ. Math. Debrecen, **41**, 1992, 289–294.

Kataoka,T. [80]: On the integer ring of the compositum of algebraic number fields, Nagoya Math. J., **77**, 1980, 25–31.

Katayama,K. [66]: Kronecker's limit formulas and their applications, J. Fac. Sci. Tokyo, **13**, 1966, 1–44.

Katayama,K. [76]: On the values of ray-class L-functions for real quadratic fields, J. Math. Soc. Japan, **28**, 1976, 455–482.

Katayama,S. [97]: On the class numbers of real quadratic fields of Richaud-Degert type, J. Math. Tokushima Univ., **31**, 1997, 1–6.

Katayama,S.I.,Katayama,S. [92]: On certain real bicyclic biquadratic fields with class number one and two, J. Math. Tokushima Univ., **26**, 1992, 1–8.

Katayama,S.I.,Katayama,S. [94]: On bounds for fundamental units of real quadratic fields, J. Number Theory, **46**, 1994, 385–390.

Kaufman,R.M. [77]: The geometric aspect of Linnik's theorem on the least prime, Lit. Mat. Sb., **17**, 1977, no.1, 111–114. (Russian)

Kaufman,R.M. [78a]: An estimate of Hecke's L-functions of the Gaussian field on the line Re $s = 1/2$, DAN Belorus. SSR, **22**, 1978, 25–82. (Russian)

Kaufman,R.M. [78b]: A.F.Lavrik's truncated equation, Zap. Nauchn. Sem. LOMI, **76**, 1978, 124–158. (Russian)

Kaufman,R.M. [79]: An evaluation of Hecke's L-functions on the critical line, Zap. Nauchn. Sem. LOMI, **91**, 1979, 40–51. (Russian)

Kawada,Y. [51]: On the derivations in number fields, Ann. of Math., (2) **54**, 1951, 302–314.

Kawada,Y. [54]: On the structure of the Galois group of some infinite extensions, J. Fac. Sci. Univ. Tokyo, I, **7**, 1954, 1–18.
Kawamoto,F. [84]: On normal integral bases, Tokyo J. Math., **7**, 1984, 221–231; Remark: **8**, 1985, p.275.
Kawamoto,F. [86]: On normal integral bases of local fields, J. Algebra, **98**, 1986, 197–199.
Kawamoto,F. [01]: On quadratic subextensions of ray class fields of quadratic fields mod $\mathfrak{p}$, J. Number Theory, **86**, 2001, 1–38.
Kempfert,H. [62]: Zum allgemeinen Hauptidealsatz, J. Reine Angew. Math., **210**, 38–64; II, **223**, 1966, 28–55.
Kenku,M.A. [70]: Determination of the even discriminants of complex quadratic fields with class-number 2, Proc. London Math. Soc., (3), **22**, 1970, 734–746.
Kennedy,R.E. [80]: Krull rings, Pacific J. Math., **89**, 1980, 131–136.
Kersey,D. [80]: Modular units inside cyclotomic units, Ann. of Math., (2) **112**, 1980, 361–380.
Khare,C. [00]: Notes of Ribet's converse to Herbrand, in: *Cyclotomic fields and related topics (Pune, 1999)*, 273–284, Pune 2000.
Kida,Y. [80]: l-extensions of CM-fields and cyclotomic invariants, J. Number Theory, **12**, 1980, 519–528.
Kida,Y. [82]: Cyclotomic Z_2-extensions of J-fields, J. Number Theory, **14**, 1982, 340–352.
Kim,H.K.,Hwang,H.J. [00]: Values of zeta functions and class number 1 criterion for the simplest cubic fields, Nagoya Math. J., **160**, 2000, 161–180.
Kim,H.K.,Leu,M.G.,Ono,T. [87]: On two conjectures on real quadratic fields, Proc. Japan Acad. Sci., **63**, 1987, 222–224.
Kim,J.M.,Oh,S.I. [00]: On the Iwasawa λ-invariants of real quadratic fields, Acta Arith., **96**, 2000, 167–174.
Kim,S. [91]: A generalization of Fröhlich's theorem to wildly ramified quaternion extensions of Q, Illinois J. Math.. **35**, 1991, 158–189.
Kim,S. [92]: The root number and Chinburg's second invariant, J. Algebra, **153**, 1992, 133–202.
Kiming,I. [94]: On the experimental verification of the Artin conjecture for 2-dimensional odd Galois representations over Q, in: *On Artin's conjecture for odd 2-dimensional representations*, 1–36, Lecture Notes in Math., **1585**, Springer 1994.
Kiming,I.,Wang,X.D. [94]: Examples of 2-dimensional, odd Galois representations of A_5-type over $\mathbb{Q}$ satisfying the Artin conjecture, in: *On Artin's conjecture for odd 2-dimensional representations*, 109–121, Lecture Notes in Math., **1585**, Springer 1994.
Kimura,N. [79b]: On the class number of real quadratic fields $Q(\sqrt{p})$ with $p \equiv 1 \pmod 4$, Tokyo J. Math., **2**, 1979, 387–396.
Kimura,T.,Horie,K. [87]: On the Stickelberger ideal and the relative class number, Trans. Amer. Math. Soc., **302**, 1987, 727–739.
King,H. [68]: Analytic representation for the L-series for certain ray characters, Comm. Pure Appl. Math., **21**, 1968, 523–533.
Kinohara,A. [52]: On the derivations and the relative differents in algebraic number fields, J. Sci. Hiroshima Univ., **16**, 1952, 261–266.
Kiselev,A.A. [48]: The expression of the class-number of ideals of real quadratic fields by Bernoulli numbers, Dokl. Akad. Nauk SSSR, **61**, 1948, 777–779. (Russian)
Kiselev,A.A. [55a]: On the class-number of ideals in cubic fields, Uchen. Zap. Leningrad. Gos. Ped. Inst., **14**, 1955, 45–61. (Russian)

Kiselev,A.A. [55b]: On a congruence relating the class-number of ideals in two quadratic fields, whose discriminants differ by a factor, Uchen. Zap. Leningr. Gos. Ped. Inst., **14**, 1955, 52–56. (Russian)

Kiselev,A.A. [59]: On certain congruences for the class-number of ideals of real quadratic fields, whose discriminants differ by a factor, Uchen. Zap. Leningr. Gos. Ped. Inst., **16**, 1959, 20–31. (Russian)

Kiselev,A.A.,Slavutskii,I.Sh. [59]: On the class-number of ideals in a quadratic field and its rings, Dokl. Akad. Nauk SSSR, **126**, 1959, 1191–1194. (Russian)

Kiselev,A.A.,Slavutskii,I.Sh. [62]: Some congruences for the number of representations by sums of an odd number of squares, Dokl. Akad. Nauk SSSR, **143**, 1962, 1191–1194. (Russian)

Kiselev,A.A.,Slavutskii,I.Sh. [64]: Transformation of Dirichlet's formulae and arithmetical computation of the class-number of ideals in quadratic fields, in : *Trudy IV Mat. S'ezda*, **II**, 1964, 105–112, Leningrad 1964. (Russian)

Kishi,Y. [00]: A constructive approach to Spiegelung relations between 3-ranks of absolute ideal class groups and congruent ones mod $(3)^2$ in quadratic fields, J. Number Theory, **83**, 2000, 1–49.

Kishi,Y.,Miyake,K. [00]: Parametrization of the quadratic fields whose class numbers are divisible by three, J. Number Theory, **80**, 2000, 209–217.

Kisilevsky,H. [70]: Some results related to Hilbert's theorem 94, J. Number Theory, **2**, 1970, 199–206.

Kisilevsky,H. [76]: Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94, J. Number Theory, **8**, 1976, 271–279.

Kisilevsky,H. [82]: The Rédei-Reichardt theorem: another proof, in: *Ternary Quadratic Forms and Norms*, 1–4, Marcel Dekker 1982.

Kisilevsky,H. [97]: A generalization of a result of Sinnott, Pacific J. Math., 1997, Special Issue, 225–229,

Kitaoka,Y. [01]: Distribution of units of a cubic field with negative discriminant, J. Number Theory, **91**, 2001, 318–355.

Kleboth,H. [55]: Untersuchungen über Klassenzahl und Reziprozitätsgesetz in Körper der $6l$-ten Einheitswurzeln und die diophantische Gleichung $X^{2l}+3^lY^{2l} = Z^{2l}$ für eine Primzahl grösser als 3, Thesis, Univ. Zürich 1955.

Kleiman,H. [71]: Totally real subfields of p-adic fields having the symmetric group as Galois group, Canad. Math. Bull., **14**, 1971, 441–442.

Klingen,N. [62]: Über die Werte der Dedekindschen Zetafunktion, Math. Ann., **145**, 1961/62, 265–277.

Klingen,N. [78]: Zahlkörper mit gleicher Primzerlegung, J. Reine Angew. Math., **299/300**, 1978, 342–384.

Klingen,N. [79]: Atomare Kronecker-Klassen mit speziellen Galoisgruppen, Abh. Math. Sem. Univ. Hamburg, **48**, 1979, 42–53.

Klingen,N. [80]: Über schwache quadratische Zerlegungsgesetze, Comment. Math. Helv., **55**, 1980, 645–651.

Klingen,N. [83]: Allgemeine Primstellen und Kroneckerklassen unendlicher Körpererweiterungen, Resultate Math., **6**, 1983, 183–193.

Klingen,N. [98]: *Arithmetical Similarities*, Oxford University Press, 1998.

Knapowski,S. [68]: On Siegel's theorem, Acta Arith., **14**, 1968, 417–424.

Knapowski,S. [69]: On a theorem of Hecke, J. Number Theory, **1**, 1969, 235–251.

Knebusch,M.,Scharlau,W. [71]: Quadratische Formen und quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern, Math. Z., **121**, 1971, 346–368.

Kneser,H. [42]: Zur Stetigkeit der Wurzeln einer algebraischen Gleichung, Math. Z., **48**, 1942, 101–104.

Kneser,M. [75]: Lineare Abhängigkeit von Wurzeln, Acta Arith., **26**, 1974/75, 307–308.

Knuth,D.E. [69]: *The Art of Computer Programming*, vol.II, Reading 1969.
Kobayashi,M. [83]: The connected component of the idéle class group of an algebraic number field, Pacific J. Math., **106**, 1983, 129–134.
Kobayashi,S. [71]: On the l-dimension of the ideal class group of Kummer extensions of a certain type, Proc. Japan Acad. Sci., **18**, 1971, 399–404.
Kobayashi,S. [74]: On the l-class rank in some algebraic number fields, J. Math. Soc. Japan, **26**, 1974, 668–676.
Kobayashi,S. [77]: Complete determination of the 3-class rank in pure cubic fields, J. Math. Soc. Japan, **29**, 1977, 373–384.
Kobayashi,S. [79]: Divisibility of class numbers of real cyclic extensions of degree 4 over Q, J. Reine Angew. Math., **307/308**, 1979, 365–372.
Kobayashi,S. [80]: Divisibilité du nombre de classes des corps abéliens réels, J. Reine Angew. Math., **320**, 1980, 142–149.
Kobayashi,S. [82]: L'indice de l'idéal de Stickelberger l-adique, Math. Z., **179**, 453–464.
Koblitz,N. [77]: *P-adic Numbers, p-adic Analysis and Zeta-functions*, Springer 1977; 2nd edition: Springer 1984.
Koch,H. [66]: Zur Begründung der Arithmetik in algebraischen Zahl- und Funktionenkörpern, Wiss. Z. Humboldt Univ. Berlin, **15**, 1966, 203–206.
Koch,H. [69]: Zum Satz von Golod-Schafarewitsch, Math. Nachr., **42**, 1969, 321–333.
Koch,H. [70]: *Galoissche Theorie der p-Erweiterungen*, Akademie-Verlag 1970. [English translation: Springer 2002.]
Koch,H. [75]: Zum Satz von Golod-Schafarewitsch, J. Reine Angew. Math., **274/275**, 1975, 240–243.
Koch,H. [90]: *Algebraic Number Theory*, Moskva 1990. (Russian) [English translation: Springer 1992.]
Koch,H. [97]: *Zahlentheorie*, Vieweg 1997. [English translation: *Number Theory*, Amer. Math. Soc. 2000.]
Koch,H.,Zink,W. [72]: Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern, Math. Nachr., **54**, 1972, 310–323.
Kohnen,W. [01]: Class numbers of imaginary quadratic fields, in: *Class Field Theory – its Centenary and Prospect (Tokyo 1998)*, 415–417, Math. Soc. Japan, 2001.
Kohnen,W.,Ono,K. [99]: Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication, Invent. math., **135**, 1999, 387–398.
Kolyvagin,V.A. [90]: Euler systems, in *The Grothendieck Festschrift*, **II**, 435–483, Birkhäuser 1990.
Komatsu,K. [74]: The Galois group of the algebraic closure of an algebraic number field, Kodai Math. Rep., **26**, 1974/75, 44–52.
Komatsu,K. [75]: Integral bases in algebraic number fields, J. Reine Angew. Math., **278/279**, 1975, 137–144.
Komatsu,K. [76a]: Discriminants in certain algebraic number fields, J. Reine Angew. Math., **285**, 1976, 114–125.
Komatsu,K. [76b]: An integral basis of the algebraic number field $Q(\sqrt[l]{a}, \sqrt[l]{1})$, J. Reine Angew. Math., **288**, 1976, 152–153.
Komatsu,K. [76c]: On the adele rings of algebraic number fields, Kodai Math. Rep., **28**, 1976, 78–84.
Komatsu,K. [78]: On the adele rings and zeta-functions of algebraic number fields, Kodai Math. J., **1**, 1978, 394–400.
Komatsu,K. [82]: On a certain property of profinite groups, Proc. Japan Acad. Sci., **58**, 1982, 319–322.

Komatsu,K. [84]: On the adèle rings of arithmetically equivalent fields, Acta Arith., **43**, 1984, 93–95.
Komatsu,K. [97]: Construction of normal bases by special values of Hilbert modular functions, Proc. Japan Acad. Sci., **73**, 1997, 42–44.
Komatsu,K. [98]: On the Z_l-extension of a certain cubic cyclic field, Proc. Japan Acad. Sci., **74**, 1998, 165–166.
Komatsu,K. [99]: On the Iwasawa λ-invariants of quaternion extensions, Acta Arith., **87**, 1999, 219–221.
Komatsu,K. [01]: A family of infinite pairs of quadratic fields $Q(\sqrt{D})$ and $Q(\sqrt{-D})$ whose class numbers are both divisible by 3, Acta Arith., **96**, 2001, 213–221.
Komatsu,K. [02]: An infinite family of pairs of quadratic fields $Q(\sqrt{D})$ and $Q(\sqrt{mD})$ whose class numbers are both divisible by 3, Acta Arith., **104**, 2002, 129–136.
Komatsu,T.,Nakano,S. [01]: On the Galois module structure of ideal class groups, Nagoya Math. J., **164**, 2001, 133–146.
König,R. [13]: Über quadratische Formen und Zahlkörper, sowie zwei Gruppensätze, Jahresber. Deutsch. Math.-Verein., **22**, 1913, 239–254.
Konno,S. [65]: On Kronecker's limit formula in a totally imaginary quadratic field over a totally imaginary field, J. Math. Soc. Japan, **17**, 1965, 412–424.
Konno,S. [88]: On Kronecker's limit formula for certain biquadratic fields, in: *Investigations in Number Theory*, 297–311, Academic Press 1988.
Koppenhöfer,D. [95]: Determining the monogeneity of a quartic number field, Manuscripta Math., **172**, 1995, 191–198.
Korchagina,V.I. [79]: The distribution of prime ideal numbers in a quadratic field, DAN Tadzhik. SSR, **22**, 1979, 152–154. (Russian)
Koshi,Y. [01]: Imaginary cyclic fields of degree $p-1$ whose relative class numbers are divisible by p, Proc. Japan Acad. Sci., **77**, 2001, 55–58.
Kostra,J. [89]: Remark on the minimum discriminant of normal fields, Czechoslov. Math. J., **39(114)**, 1989, 555–558.
Kostra,J. [94]: On sums of two units, Abh. Math. Sem. Univ. Hamburg, **64**, 1994, 11–14.
Kostrikin,A.J. [65]: Defining groups by generators and relations, Izv. Akad. Nauk SSSR, Ser. Mat., **29**, 1965, 1119–1122. (Russian)
Kovalchik,F.B. [74]: Density theorems and the distribution of primes in sectors and progressions, Dokl. Akad. Nauk SSSR, **219**, 1974, 31–34. (Russian)
Kovalchik,F.B. [75]: On a generalization of the Halász-Montgomery method, Lit. Mat. Sb., **15**, 1975, no.3, 139–149. (Russian)
Kovács,B. [81]: Canonical number systems in algebraic number fields, Acta Math. Acad. Sci. Hungar., **37**, 1981, 405–407.
Kovács,B.,Pethö,A. [91]: Number systems in integral domains, especially in orders of algebraic number fields, Acta Sci. Math. (Szeged), **55**, 1991, 287–299.
Kovács,B.,Pethö,A. [92]: On a representation of algebraic integers, Studia Sci. Math. Hungar., **27**, 1992, 169–172.
Koyama,T., Nishi,M., Yanagihara,H. [74]: On characterizations of Dedekind domains, Hiroshima Math. J., **4**, 1974, 71–74.
Kraft,J.S. [89]: Iwasawa invariants of CM fields, J. Number Theory, **32**, 1989, 65–77.
Kraft,J.S. [96]: Class numbers and Iwasawa invariants for quadratic fields, Proc. Amer. Math. Soc., **124**, 1996, 31–34.
Kraft,J.S.,Schoof,R. [95]: Computing Iwasawa invariants of real quadratic fields, Compositio Math., **97**, 1995, 135–155.
Krakowski,F. [65]: On the content of polynomials, Proc. Amer. Math. Soc., **16**, 1965, 810–812.

Kramer,D. [87]: On the values at integers of the Dedekind zeta function of a real quadratic field, Trans. Amer. Math. Soc., **299**, 1987, 59–79.

Krasner,M. [35]: Sur la théorie de la ramification des idéaux, C.R. Acad. Sci. Paris, **200**, 1935, 1813–1815.

Krasner,M. [36]: Sur la représentation multiplicative dans les corps de nombres P-adiques relativement galoisiens, C.R. Acad. Sci. Paris, **203**, 1936, 907–908.

Krasner,M. [37a]: Définition de certains anneaux non commutatifs. Classification des extensions primitives des corps à valuation discréte, C.R. Acad. Sci. Paris, **205**, 1937, 772–774; corr., p.1111, 1347–1348; **206**, 1938, p.288.

Krasner,M. [37b]: Le nombre des surcorps d'un degré donné d'un corps de nombres $\mathfrak{p}$-adiques, C.R. Acad. Sci. Paris, **205**, 1937, 1026–1028; corr. p.1267.

Krasner,M. [37c]: Sur la primitivité des corps P-adiques, Mathematica, **13**, 1937, 72–191.

Krasner,M. [38]: Le nombre des surcorps primitifs d'un degré donné et le nombre des surcorps métagaloisiens d'un degré donné d'un corps de nombres $\mathfrak{p}$-adiques, C.R. Acad. Sci. Paris. **206**, 1938, 876–878; corr. p.1152.

Krasner,M. [39]: Sur la représentation exponentielle dans les corps relativement galoisiens de nombres $\mathfrak{p}$-adiques, Acta Arith., **3**, 1939, 133–173.

Krasner,M. [46]: Théorie non abélienne des corps de classes pour les extensions finies et séparables des corps valués complets, C.R. Acad. Sci. Paris, **222**, 1946, 626–628, 984–986, 1370–1372; **224**, 1947, 173–175, 434–436.

Krasner,M. [47]: Théorie non-abélienne des corps de classes pour les extensions galoisiennes des corps de nombres algébriques, C.R. Acad. Sci. Paris, **225**, 1947, 785–787, 973–975, 1113–1115; **226**, 1948, 535–537, 1231–1233, 1656–1658.

Krasner,M. [62]: Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique, C.R. Acad. Sci. Paris, **254**, 1962, 3470–3472; **255**, 1962, 224–226, 1682–1684, 2342–2344, 3095–3097.

Krasner,M. [66]: Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique, in: *Les tendances géometriques en algébre et théorie des nombres*, 143–169, Paris 1966.

Krasner,M. [79]: Remarques au sujet d'une note de J.P.Serre, C.R. Acad. Sci. Paris, **288**, 1979, A863–865.

Krause,U. [84]: A characterization of algebraic number fields with cyclic class groups of prime power order, Math. Z., **186**, 1984, 143–148.

Krause,U.,Zahlten,C. [91]: Arithmetic in Krull monoids and the cross number of divisor class groups, Mitt. Math. Ges. Hamburg, **12**, 1991, 681–696.

Kronecker,L. [45a]: *De unitatibus complexis*, Berlin 1845 = *Werke*, **I**, 5–73, Leipzig 1895.

Kronecker,L. [45b]: Beweis, dass für jede Primzahl p die Gleichung $1 + x + x^2 + \ldots + x^{p-1} = 0$ irreduzibel ist, J. Reine Angew. Math., **29**, 1845, p.280 = *Werke*, **I**, 3–4, Leipzig 1895.

Kronecker,L. [53]: Über die algebraisch auflösbaren Gleichungen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1853, 365–374; 1856, 203–215 = *Werke*, **IV**, 1–11, 25–37, Leipzig-Berlin 1929.

Kronecker,L. [54]: Mémoire sur les facteurs irréductiblés de l'expression $x^n - 1$, J. math. pures appl., **19**, 1854, 177–192 = *Werke*, **I**, 75–92. Leipzig 1895.

Kronecker,L. [56a]: Démonstration d'un théorème de M. Kummer, J. math. pures appl., (2) **1**, 396–398 = *Werke*, **I**, 93–97, Leipzig 1895.

Kronecker,L. [56b]: Démonstration de l'irréductibilité de l'équation $x^{n-1} + x^{n-2} + \ldots + 1 = 0$ ou n désigne un nombre premier, J. math. pures appl., (2) **1**, 1856, 399–400 = *Werke*, **I**, 99–102, Leipzig 1895.

Kronecker,L. [57a]: Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, J. Reine Angew. Math., **53**, 1857, 173–175 = *Werke*, **I**, 103–108, Leipzig 1895.

Kronecker,L. [57b]: Über complexe Einheiten, J. Reine Angew. Math., **53**, 1857, 176–181 = *Werke*, **I**, 109–118, Leipzig 1895.

Kronecker,L. [63]: Über die Klassenzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1863, 340–341 = *Werke*, **I**, 123–131, Leipzig 1895.

Kronecker,L. [64]: Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1864, 285–303 = *Werke*, **IV**, 227–244, Leipzig-Berlin 1929.

Kronecker,L. [77]: Über Abelsche Gleichungen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1877, 845–851 = *Werke*, **IV**, 63–71, Leipzig-Berlin 1929.

Kronecker,L. [80]: Über die Irreduktibilität der Gleichungen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1880, 155–163 = *Werke*, **II**, 85–93, Leipzig 1897.

Kronecker,L. [82]: Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. Reine Angew. Math., **92**, 1882, 1–122 = *Werke*, **II**, 237–387, Leipzig 1897.

Kronecker,L. [83]: Sur les unités complexes, C.R. Acad. Sci. Paris, **96**, 1883, 93–98, 148–152, 216–222 = *Werke*, $\mathbf{III}_1$, 1–20, Leipzig 1899.

Kronecker,L. [84]: Additions au mémoire sur les unités complexes, C.R. Acad. Sci. Paris, **99**, 1884, 765–771 = *Werke*, $\mathbf{III}_1$, 21–30, Leipzig 1899.

Kronecker,L. [85]: Zur Theorie der elliptischen Funktionen, SBer. Kgl. Preuß. Akad. Wiss. Berlin, 1885, 761–784; 1889, 123–135 = *Werke*, **IV**, 363–389, 482–495, Leipzig-Berlin 1929.

Krull,W. [28a]: Zur Theorie der allgemeinen Zahlringen, Math. Ann., **98**, 1928, 51–70.

Krull,W. [28b]: Idealtheorie in unendlichen Zahlkörpern, Math. Z., **29**, 1928, 42–54; II, **31**, 1930, 527–557.

Krull,W. [28c]: Zur Theorie der allgemeinen Zahlringe, Math. Ann., **99**, 1928, 51–70.

Krull,W. [28d]: Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., **100**, 1928, 687–698.

Krull,W. [30]: Ein Hauptsatz über umkehrbare Ideale, Math. Z., **31**, 1930, p.558.

Krull,W. [31]: Allgemeine Bewertungstheorie, J. Reine Angew. Math., **167**, 1931, 160–196.

Krull,W. [35]: *Idealtheorie*, Springer 1935.

Krull,W. [51]: Zur Arithmetik der endlichen diskreten Hauptordnungen, J. Reine Angew. Math., **189**, 1951, 118–128.

Kubert,D. [85]: Jacobi sum and Hecke characters, Amer. J. Math., **107**, 1985, 253–280.

Kubert,D. [86]: The 2-divisibility of the class number of cyclotomic fields and the Stickelberger ideal, J. Reine Angew. Math., **369**, 1986, 192–218.

Kubert,D.,Lang,S. [79]: Modular units inside cyclotomic units, Bull. Soc. Math. France, **107**, 1979, 161–178.

Kubert,D.,Lang,S. [81]: *Modular Units*, Springer 1981.

Kubert,D.,Lichtenbaum,S. [83]: Jacobi-sum Hecke characters and Gauss sum identities, Compositio Math., **48**, 1983, 55–87.

Kubilius,J. [52]: On certain problems of the geometry of numbers, Mat. Sb., **31**, 1952, 507–542. (Russian)

Kubota,K.K.,Liardet,P. [72a]: Note on a conjecture of W.Narkiewicz, J. Number Theory, **4**, 1972, 181–190.

Kubota,T. [56a]: Density in a family of abelian extensions, in: *Proceedings of the International Symposium on Algebraic Number Theory*, 77–91. Tokyo 1956.

Kubota,T. [56b]: Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J., **10**, 1956, 65–85.

Kubota,T. [57]: Galois group of the maximal abelian extension over an algebraic number field, Nagoya Math. J., **12**, 1957, 177–189.

Kubota,T. [60]: Local relation of Gauss sums, Acta Arith., **6**, 1960/61, 285–294.

Kubota,T. [61]: Über quadratische Charaktersummen, Nagoya Math. J., **19**, 1961, 15–25.

Kubota,T. [63]: Über eine Verallgemeinerung der Reziprozität der Gaussschen Summen, Math. Z., **82**, 1963, 91–100.

Kubota,T.,Leopoldt,H.W. [64]: Eine p-adische Theorie der Zetawerte, I, J. Reine Angew. Math., **215/215**, 1964, 328–339.

Kubotera,N. [00]: Greenberg's conjecture and Leopoldt's conjecture, Proc. Japan Acad. Sci., **76**, 2000, 108–110.

Kučera,R. [97]: A note on Sinnott's definition of circular units of an abelian field, J. Number Theory, **63**, 1997, 403–407.

Kučera,R. [01]: Formulae for the relative class number of an imaginary abelian field in the form of a determinant, Nagoya Math. J., **163**, 2001, 167–191.

Kudo,A. [72]: On the reflection theorem in prime cyclotomic fields, Mem. Fac. Sci. Kyushu Univ., A **26**, 1972, 333–337.

Kudo,A. [75a]: On a generalization of a theorem of Kummer, Mem. Fac. Sci. Kyushu Univ., A, **29**, 1975, 255–261.

Kudo,A. [75b]: On a class number relation of imaginary abelian fields, J. Math. Soc. Japan, **27**, 1975, 150–159.

Kühnova,J. [79]: Maillet's determinant $D_{p^{n+1}}$, Arch. Math. (Brno), **15**, 1979, 209–212.

Kulkarni,R.S. [67]: On a theorem of Jensen, Amer. Math. Monthly, **74**, 1967, 960–961.

Kummer,E.E. [42]: Eine Aufgabe betreffend die Theorie der cubischen Reste, J. Reine Angew. Math., **23**, 1842, 285–286 = *Collected Papers*, **I**, 143–144, Springer 1975.

Kummer,E.E. [46]: De residuis cubicis disquisitiones nonnullae analyticae, J. Reine Angew. Math., **32**, 1846, 341–359 = *Collected Papers*, **I**, 145–163, Springer 1975.

Kummer,E.E. [47a]: Zur Theorie der complexen Zahlen, J. Reine Angew. Math., **35**, 1847, 319–325 = *Collected Papers*, **I**, 203–210, Springer 1975.

Kummer,E.E. [47b]: Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfaktoren, J. Reine Angew. Math., **35**, 1847, 327–367 = *Collected Papers*, **I**, 211–251, Springer 1975.

Kummer,E.E. [50a]: Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ-ten Wurzeln der Einheit gebildeten complexen Zahlen und die ideale Faktoren derselben, J. Reine Angew. Math., **40**, 1850, 93–116 = *Collected Papers*, **I**, 299–322, Springer 1975.

Kummer,E.E. [50b]: Zwei besondere Untersuchungen über die Classen Anzahl und über die Einheiten der aus den λ-ten Wurzeln der Einheit gebildeten complexen Zahlen, J. Reine Angew. Math., **40**, 1850, 117–129 = *Collected Papers*, **I**, 332–335, Springer 1975.

Kummer,E.E. [50c]: Allgemeiner Beweis des Fermatschen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenige Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoulli'schen Zahlen nicht vorkommen, J. Reine Angew. Math., **40**, 1850, 130–138 = *Collected Papers*, **I**, 336–344, Springer 1975.

Kummer,E.E. [51]: Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers, J. math. pures appl., **16**, 1851, 377–498 = *Coll. Papers*, **I**, 363–484, Springer 1975.

Kummer,E.E. [56]: Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, Abh. Kgl. Preuß. Akad. Wiss. Berlin, 1856, 1–47 = *Coll. Papers*, **I**, 583–629, Springer 1975.

Kummer,E.E. [57]: Einige Sätze über die aus der Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen für den Fall, dass die Classenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermatschen Satzes, Abh. Kgl. Preuß. Akad. Wiss. Berlin, 1857, 41–74 = *Collected Papers*, **I**, 639–672, Springer 1975.

Kummer,E.E. [59]: Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist, Abh. Kgl. Preuß. Akad. Wiss. Berlin, 1859, 19–159 = *Collected Papers*, **I**, 699–839, Springer 1975.

Kummer,E.E. [61]: Über die Classenanzahl der aus n-ten Einheitswurzeln gebildeten complexen Zahlen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1861, 1051–1053 = *Collected Papers*, **I**, 883–885, Springer 1975.

Kummer,E.E. [63]: Über die Classenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen complexen Zahlen, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1863, 21-28 = *Collected Papers*, **I**, 887–894, Springer 1975.

Kummer,E.E. [70]: Über die Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen und über den zweiten Faktor der Classenzahl, Mon. Ber. Kgl. Preuß. Akad. Wiss., 1870, 855–880 = *Collected Papers*, **I**, 919–944, Springer 1975.

Kunert,D. [35]: Ein neuer Beweis für die Reziprozitätsformel der Gaussschen Summen in beliebigen quadratischen Zahlkörpern, Math. Z., **40**, 1935, 326–347.

Kuniyoshi,H.,Takahashi,S. [53]: On the principal genus theorem, Tôhoku Math. J., (2) **10**, 1953, 128–131.

Kurihara,M. [92]: Some remarks on conjectures about cyclotomic fields and K-groups of Z, Compositio Math., **81**, 1992, 223–236.

Kuroda,S. [43]: Über den Dirichletschen Körper, J. Fac. Sci. Univ. Tokyo, **4**, 1943, 383–406.

Kuroda,S. [50]: Über die Klassenzahlen algebraischer Zahlkörper, Nagoya Math. J., **1**, 1950, 1–10.

Kuroda,S. [51]: Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, J. Math. Soc. Japan, **3**, 1951, 148–156.

Kuroda,S.-N. [62]: On a theorem of Minkowski, Sûgaku, **14**, 1962/63, 171–172. (Japanese)

Kuroda,S.-N. [64a]: On the class number of imaginary quadratic number fields, Proc. Japan Acad. Sci., **40**, 1964, 365–367.

Kuroda,S.-N. [64b]: Über die Klassenzahl eines relativzyklischen Zahlkörpers vom Primzahlgrade, Proc. Japan Acad. Sci., **40**, 1964, 623–626.

Kuroda,S.-N. [70]: Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper, J. Number Theory, **2**, 1970, 282–297.

Kurokawa,N. [78a]: On the meromorphy of Euler products, Proc. Japan Acad. Sci., **54**, 1978, 163–166.

Kurokawa,N. [78b]: On Linnik's problem, Proc. Japan Acad. Sci., **54**, 1978, 167–169.

Kurokawa,N. [86]: On the meromorphy of Euler products, I, II, Proc. London Math. Soc., (3) **53**, 1986, 1–47, 209–236.

Kürschak,J. [13]: Über Limesbildung und allgemeine Körpertheorie, J. Reine Angew. Math., **142**, 1913, 211–253.

Kutsuna,M. [74]: On the fundamental units of real quadratic fields, Proc. Japan Acad. Sci., **50**, 1974, 580–583.

Kutsuna,M. [80]: On a criterion for the class number of a quadratic field to be one, Nagoya Math. J., **79**, 1980, 123–129.
Kuzmin,L.V. [69]: Homologies of profinite groups, the Schur multiplier and class field theory, Izv. Akad. Nauk SSSR, Ser. Mat., **33**, 1969, 1220–1254. (Russian)
Kuzmin,L.V. [81]: Some remarks on l-adic Dirichlet theorem and the l-adic regulator, Izv. Akad. Nauk SSSR, Ser. Mat., **45**, 1981, 1203–1240. (Russian)
Kuzmin,L.V. [96]: On formulas for the class number of real abelian fields, Izv. Ross. Akad. Nauk, Ser. Mat., **60**, No.4, 1996, 43–110. (Russian)
Kwon,S.H. [84]: Corps de nombres de degré 4 de type alterné, C.R. Acad. Sci. Paris, **209**, 1984, 41–43.
Kwon,S.H. [96]: Sur les discriminants minimaux des corps quaternioniens, Archiv Math., **67**, 1996, 119–125.
Lachaud,G. [87]: On real quadratic fields, Bull. Amer. Math. Soc., (N.S.) **17**, 1987, 307–311.
Lafon,J.P. [71]: Anneaux locaux commutatifs sur lequels tout module de type fini est somme directe de modules monogènes, J. Algebra, **17**, 1971, 575–591.
Lagarias,J.C. [78]: Signatures of units and congruences (mod 4) in certain real quadratic fields, J. Reine Angew. Math., **301**, 1978, 142–146; II, **320**, 1980, 115–126.
Lagarias,J.C. [80a]: On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc., **260**, 1980, 485–508.
Lagarias,J.C. [80b]: Signatures of units and congruences (mod 4) in certain totally real fields, J. Reine Angew. Math., **320**, 1980, 1–5.
Lagarias,J.C. [80c]: On determining the 4-rank of the ideal class group of a quadratic field, J. Number Theory, **12**, 1980, 191–196.
Lagarias,J.C.,Lenstra,H.W.Jr. [81]: Problem A6341, Amer. Math. Monthly, **88**, 1981, 294.
Lagarias,J.C.,Montgomery.H.L.,Odlyzko,A. [79]: A bound for the least prime ideal in the Chebotarev density theorem, Invent. math., **54**, 1979, 271–296.
Lagarias,J.C.,Odlyzko,A. [77]: Effective versions of the Chebotarev density theorem, in: *Algebraic Number Fields*, 409–464, London 1977.
Lagarias,J.C.,Odlyzko,A. [79]: On computing Artin L-functions in the critical strip, Math. Comp., **33**, 1979, 1081–1085.
Lagrange,J.L. [66]: Solution d'un problème d'arithmétique, Misc. Taurinensis, **4**, 1766/69 = *Oeuvres*, **I**, 671–731, Paris 1867.
Lagrange,J.L. [73]: Recherches d'arithmétique, N. Mém, Acad. Roy. Sci. Bell. Lettr. de Berlin, 1773, 1775 = *Oeuvres*, **III**, 695–795, Paris 1869.
Lai,D.T. [65]: On the number of divisors in angles, Mat. Sb., **67**,1965, 345–365. (Russian)
Lakein,R.B. [69]: A Gauss bound for a class of biquadratic fields, J. Number Theory, **1**, 1969, 108–112.
Lakkis,K. [66a]: Die galoischen Gaussschen Summen von Hasse, Bull. Soc. Math. Grèce, **7**, 1966, 183–371.
Lakkis,K. [66b]: Die verallgemeinerten Gaussschen Summen, Archiv Math., **17**, 1966, 505–509.
Lakkis,K. [67]: Die lokalen verallgemeinerten Gaussschen Summen, Bull. Soc. Math. Grèce, **8**, 1967, 143–150.
Lamprecht,E. [53]: Allgemeine Theorie der Gausschen Summen in endlichen kommutativen Ringen, Math. Nachr., **9**, 1953, 149–196.
Lamprecht,E. [57]: Struktur und Relationen allgemeiner Gaussscher Summen in endlichen Ringen, I,II, J. Reine Angew. Math., **197**, 1957, 1–26, 27–48.

Lamprecht,E. [67]: Existenz von Zahlkörpern mit nicht abbrechenden Klassenkörperturm, Archiv Math., **18**, 1967, 140–152.

Lánczi,E. [65]: Unique factorization in imaginary quadratic fields, Ann. Univ. Sci. Budapest, **16**, 1965, 453–466; add.: **26**, 1983, 195–196.

Landau,E. [03a]: Ueber die zu einem algebraischen Zahlkörper gehörige Zetafunction und die Ausdehnung der Tschebyscheffschen Primzahlentheorie auf das Problem der Verteilung der Primideale, J. Reine Angew. Math., **125**, 1903, 64–188.

Landau,E. [03b]: Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, Math. Ann., **56**, 1903, 645–670.

Landau,E. [03c]: Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante, Math. Ann., **56**, 1903, 671–676.

Landau,E. [04]: Über die Darstellung der Anzahl der Idealklassen eines algebraischen Körpers durch eine unendliche Reihe, J. Reine Angew. Math., **127**, 1904, 167–174.

Landau,E. [07]: Über die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers, Math. Ann., **63**, 1907, 145–204.

Landau,E. [08]: Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestanzahl der zu ihrer additiver Zusmmensetzung erforderlichen Quadrate, Arch. Math. Phys., (3) **13**, 1908, 305–312.

Landau,E. [12a]: Über die Anzahl der Gitterpunkte in gewisser Bereichen, Nachr. Ges. Wiss. Göttingen, 1912, 687–771.

Landau,E. [12b]: Über eine idealtheoretische Funktion, Trans. Amer. Math. Soc., **13**, 1912, 1–21.

Landau,E. [18a]: Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen, Nachr. Ges. Wiss. Göttingen, 1918, 79–97.

Landau,E. [18b]: Über imaginärquadratische Zahlkörper mit gleicher Klassenzahl, Nachr. Ges. Wiss. Göttingen, 1918, 277–284.

Landau,E. [18c]: Über die Klassenzahl imaginärquadratischer Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1918, 285–296.

Landau,E. [18d]: Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper, Nachr. Ges. Wiss. Göttingen, 1918, 478–488.

Landau,E. [18e]: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und Ideale*, Leipzig 1918; 2nd ed. 1927. [Reprint: Chelsea 1949.]

Landau,E. [18f]: Über Ideale und Primideale in Idealklassen, Math. Z., **2**, 1918, 52–154.

Landau,E. [19a]: Zur Theorie der Heckeschen Zetafunktionen, welche komplexen Charakteren entsprechen, Math. Z., **4**, 1919, 152–162.

Landau,E. [19b]: Über die Wurzeln der Zetafunktion eines algebraischen Zahlkörpers, Math. Ann., **79**, 1919, 388–401.

Landau,E. [22]: Der Minkowskische Satz über die Körperdiskriminante, Nachr. Ges. Wiss. Göttingen, 1922, 80–82.

Landau,E. [24a]: Über die Wurzeln des Zetafunktion, Math. Z., **20**, 1924, 98–104.

Landau,E. [24b]: Über die Anzahl der Gitterpunkte in gewisser Bereichen, IV, Nachr. Ges. Wiss. Göttingen, 1924, 137–150.

Landau,E. [25]: Bemerkungen zu der Arbeit des Herrn Walfisz: "Über das Piltzsche Problem in algebraischen Zahlkörpern", Math. Z., **22**, 1925, 189–205.

Landau,E. [27a]: *Vorlesungen über Zahlentheorie*, Leipzig 1927. [Reprint: Chelsea 1969.]

Landau,E. [27b]: Über Dirichletsche Reihen mit komplexen Charakteren, J. Reine Angew. Math., **157**, 1927, 26–32.

Landau,E. [29]: Über die Irreduzibilität der Kreisteilungsgleichung, Math. Z., **29**, 1929, p.462.

Landau,E. [36]: Bemerkungen zum Heilbronnschen Satz, Acta Arith., **1**, 1936, 1–18.

Landherr,W. [36]: Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **11**, 1936, 245–248.

Landsberg,G. [97]: Ueber das Fundamentalsystem und die Diskriminante der Gattungen algebraischer Zahlen welche aus Wurzelgrössen gebildet sind, J. Reine Angew. Math., **117**, 1897, 140–147.

Lang,H. [68]: Über eine Gattung elementararithmetischer Klasseninvarianten reellquadratischer Zahlkörper, J. Reine Angew. Math., **233**, 1968, 123–175.

Lang,H. [72]: Über Anwendung höheren Dedekindscher Summen auf die Struktur elementar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper, J. Reine Angew. Math., **254**, 1972, 17–32.

Lang,H. [73a]: Über Bernoullische Zahlen in reell-quadratischen Zahlkörpern, Acta Arith., **22**, 1973, 423–437.

Lang,H. [73b]: Über verallgemeinerte Bernoullische Zahlen und die Klassenzahl reell-quadratischer Zahlkörper, Acta Arith., **23**, 1973, 13–18.

Lang,H. [76]: Über einfache periodische Kettenbrüche und Vermutungen von P.Chowla und S.Chowla, Acta Arith., **8**, 1975/76, 419–428.

Lang,H. [77]: Über die Klassenzahl der Ringklassenkörper mit einem reellquadratischen Grundkörper, Math. Ann., **227**, 1977, 127–133.

Lang,H. [85a]: Über die Klassenzahl quadratischer Zahlkörper, deren Diskriminanten nur ungerade Primtelier $p \equiv 1 \pmod 4$ besitzen, Abh. Math. Sem. Univ. Hamburg, **55**, 1985, 147–150.

Lang,H. [85b]: Über die Werte $\zeta(2-p, \mathfrak{K})$ der Zetafunktion einer Idealklasse aus einem reell-quadratischen Zahlkörper, J. Reine Angew. Math., **361**, 1985, 35–46.

Lang,H. [88]: Über die Restklasse modulo 2^{e+2} des Wertes $2^e n\zeta(1-2^e n, \mathfrak{K})$ der Zetafunktion einer Idealklasse aus dem reell-quadratischewn Zahlkörper $Q(\sqrt{D})$ mit $D \equiv 3 \pmod 4$, Acta Arith., **51**, 1988, 277–292.

Lang,H.,Schertz,R. [76]: Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper, J. Number Theory, **8**, 1976, 352–365.

Lang,S. [60]: Integral points on curves, Inst. Hautes Études Sci., Publ. Math., No.6, 1960, 27–43.

Lang,S. [64]: *Algebraic Numbers*, Reading 1964.

Lang,S. [70]: *Algebraic Number Theory*, Addison-Wesley 1970; 2nd ed. Springer 1994.

Lang,S. [71]: On the zeta functions of algebraic number fields, Invent. math., **12**, 1971, 337–345.

Lang,S. [78]: *Cyclotomic Fields, I,II*, Springer 1978; 2nd ed. 1990.

Lang,S. [82]: Units and classs groups in number theory and algebraic geometry, Bull. Amer. Math. Soc., (N.S.) **6**, 1982, 253–316.

Lang,S.D. [77]: Note on the class number of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., **290**, 1977, 70–72.

Langevin,M. [86]: Minorations de la maison et de la mesure de Mahler de certains nombres algébriques, C.R. Acad. Sci. Paris, **303**, 1986, 523–526.

Langevin,M. [88a]: Solution des problémes de Favard, Ann. Inst. Fourier, **38**, 1988, no.2, 1–10.

Langevin,M. [88b]: Solution et histoire d'un probléme de Favard, Sém. de Théorie des Nombres, Paris, 1986–87, 221–269, Progr. Math., **75**, Birkhäuser 1988.

Langevin,M. [88c]: Probléme de Favard pour les corps quadratiques imaginaires et majoration des discriminants, C.R. Acad. Sci. Paris, **307**, 1988, 427–429.

Langevin,M.,Reyssat,E.,Rhin,G. [88]: Diamètres transfinis et problème de Favard, Ann. Inst. Fourier, **38**, 1988, no.1, 1–16.
Langlands,R.M. [70]: On Artin's L-functions, in: *Complex Analysis*, Rice Univ. St., **56**, 1970, 23–28.
Lardon,R. [71]: Évaluations asymptotiques concernant la fonction Ω dans certains semi-groupes normés à factorisation unique, C.R. Acad. Sci. Paris, **273**, 76–79.
Larsen,M.D.,McCarthy,P.J. [71]: *Multiplicative Theory of Ideals*, Academic Press 1971.
Lasker,E. [05]: Zur Theorie der Moduln und Ideale, Math. Ann., **60**, 1905, 20–116.
Lasker,E. [16]: Über eine Eigenschaft der Diskriminante, Sitz. Ber. Math. Ges. Berlin, **15**, 1916, 176–178.
Latham,J. [73]: On sequences of algebraic integers, J. London Math. Soc., (2) **6**, 1973, 555–560.
Latimer,C.G. [29]: On the prime ideals of a general cubic Galois field, Amer. J. Math., **51**, 1929, 295–304.
Latimer,G. [33]: On the class-number of a cyclic field and a subfield, Bull. Amer. Math. Soc., **39**, 1933, 115–118.
Latimer,C.G. [34]: On the units in a cyclic field, Amer. J. Math., **56**, 1934, 69–74.
Latimer,C.G.,McDuffee,C.C. [33]: A correspondence between classes of ideals and classes of matrices, Ann. of Math., (2) **34**, 1933, 313–316.
Laumon,G.,Rapoport,M.,Stuhler,U. [93]: D-elliptic sheaves and the Langlands correspondence, Invent. math., **113**, 1993, 217–238.
Laurinčikas,A. [96]: *Limit Theorems for the Riemann Zeta-Function*, Kluwer 1996.
Lavrik,A.F. [59]: On the problem of distribution of the values of class-numbers of purely radical quadratic forms with negative determinant, Izv. Akad. Nauk Uzbek. SSR, 1959, no.1, 81–90. (Russian)
Lavrik,A.F. [68]: Approximate functional equations of Dirichlet functions, Izv. Akad. Nauk SSSR, Ser. Mat., **32**, 1968, 134–185. (Russian)
Lavrik,A.F. [70]: A note on the Siegel-Brauer theorem concerning parameters of algebraic number fields, Mat. Zametki, **8**, 1970, 259–263. (Russian)
Lavrik,A.F. [71a]: On moments of the class-number of purely radical quadratic forms with negative determinant, Dokl. Akad. Nauk SSSR, **197**, 1971, 32–35. (Russian)
Lavrik,A.F. [71b]: A method of evaluation of double sums with a real quadratic character and its applications, Izv. Akad. Nauk SSSR, Ser. Mat., **35**, 1971, 1189–1207. (Russian)
Lavrik,A.F.,Edgorov.Zh. [75]: The product of the number of divisor classes by the regulator of an algebraic number field, Izv. Akad. Nauk Uzbek.SSR, 1975, no.2, 77–79. (Russian)
Le,M.H. [94]: Upper bounds for class numbers of real quadratic fields, Acta Arith., **68**, 1994, 141–144.
Le,M.H. [95]: A lower bound for the class number of abelian algebraic number fields with odd degree, Proc. Amer. Math. Soc., **123**, 1995, 1347–1350.
Lebesgue,V.A. [59]: Démonstration de l'irréductibilité de l'équation aux racines primitives de l'unité, J. math. pures appl., (2) **4**, 1859, 105–110.
Ledermann,W.,van der Ploeg,C. [85]: Integral bases of dihedral number fields, I, J. Austral. Math. Soc., **38**, 1985, 351–377.
Lednev,N.A. [39]: On units of relatively cyclic algebraic fields, Mat. Sb., **6**, 1939, 227–261. (Russian)
Lee,K.C. [79]: On the average order of characters in totally real algebraic number fields, Chinese J. Math., **7**, 1979, 77–90.
Lee,Y. [02]: Cohen-Lenstra heuristics and the Spiegelungssatz: number fields, J. Number Theory, **92**, 2002, 37–66.

Leedham-Green,C.R. [72]: The classgroup of Dedekind domains, Trans. Amer. Math. Soc., **163**, 1972, 493–500.

Leep,D.B.,Wadsworth,A.R. [89]: The transfer ideal of quadratic forms and a Hasse norm theorem mod squares, Trans. Amer. Math. Soc., **315**, 1989, 415–432.

Leep,D.B.,Wadsworth,A.R. [92]: The Hasse norm theorem mod squares, J. Number Theory, **42**, 1992, 337–348.

Lefeuvre,Y. [00]: Corps diédraux à multiplication complexe principaux, Ann. Inst. Fourier, **50**, 2000, 67–103.

Lefeuvre,Y.,Louboutin,S. [00]: The class number one problem for the dihedral CM-fields, *Algebraic Number Theory and Diophantine Analysis*, (Graz 1998), 249–275, de Gruyter 2000.

Legendre,A.M. [98]: *Théorie des nombres*, Paris 1798.

Lehmer,D.H. [26]: A list of errors in tables of the Pell equation, Bull. Amer. Math. Soc., **32**, 1926, 545–550.

Lehmer,D.H. [32]: Quasi-cyclotomic poynomials, Amer. Math. Monthly, **39**, 1932, 383–389.

Lehmer,D.H. [33a]: Factorization of certain cyclotomic functions, Ann. of Math., (2) **34**, 1933, 461–479.

Lehmer,D.H. [33b]: On imaginary quadratic number fields whose class-number is unity, Bull. Amer. Math. Soc., **39**, 1933, p.360.

Lehmer,D.H. [36]: An extension of the table of Bernoulli numbers, Duke Math. J., **2**, 1936, 460–464.

Lemmermeyer,F. [89]: *Euklidische Ringe*, Diplomarbeit, Univ. Heidelberg 1989.

Lemmermeyer,F. [94a]: On 2-class fields towers of imaginary quadratic number fields, J. Théor. Nombres Bordeaux, **6**, 1994, 261–272.

Lemmermeyer,F. [94b]: Kuroda's class number formula, Acta Arith., **66**, 1994, 245–260.

Lemmermeyer,F. [95a]: Ideal class groups of cyclotomic number fields, I, Acta Arith., **72**, 1995, 347–359; II, Acta Arith., **84**, 1998, 59–70.

Lemmermeyer,F. [95b]: The Euclidean algorithm in algebraic number fields, Exposition Math., **13**, 1995, 385–416.

Lemmermeyer,F. [97a]: On 2-class field towers of some imaginary quadratic number fields, Abh. Math. Sem. Univ. Hamburg, **67**, 1997, 205–214.

Lemmermeyer,F. [97b]: Gauss bounds of quadratic extensions, Publ. Math. Debrecen, **50**, 1997, 365–368.

Lemmermeyer,F. [00]: *Reciprocity Laws*, Springer 2000.

Lemmermeyer,F. [03]: Galois action on class groups, J. Algebra, **264**, 2003, 553–564.

Lemmermeyer,F.,Louboutin,S.,Okazaki,R. [99]: The class number one problem for some non-abelian normal CM-fields of degree 24, J. Théor. Nombres Bordeaux, **11**, 1999, 387–406.

Lemmlein,V.G. [54]: On Euclidean rings and principal ideal rings, Dokl. Akad. Nauk SSSR, **97**, 1954, 585–587. (Russian)

Lenstra,H.W.Jr. [77a]: Euclidean fields of large degree, Invent. math., **38**, 1977, 237–254.

Lenstra,H.W.Jr. [77b]: On Artin's conjecture and Euclid's algorithm in global fields, Invent. math., **42**, 1977, 201–224.

Lenstra,H.W.Jr.,Stevenhagen,P. [91]: Primes of degree one and algebraic cases of Čebotarev's theorem, Enseign. Math., (2) **37**, 1991, 17–30.

Leonard,P.A.,Williams,K.S. [82]: On the divisibility of the class numbers of $Q(\sqrt{-p})$ and $Q(\sqrt{-2p})$ by 16, Canad. Math. Bull., **25**, 1982, 200–206.

Leopoldt,H.-W. [53a]: Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., **9**, 1953, 350–362.

Leopoldt,H.-W. [53b]: Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsch. Akad. Wiss., 1953, no.2, 1–48.
Leopoldt,H.-W. [58]: Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. Reine Angew. Math., **199**, 1958, 165–174.
Leopoldt,H.-W. [59]: Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., **201**, 1959, 119–149.
Leopoldt,H.-W. [61]: Zur Approximation des p-adischen Logarithmus, Abh. Math. Sem. Univ. Hamburg, **25**, 1961/62, 77–81.
Leopoldt,H.-W. [62]: Zur Arithmetik in abelschen Zahlkörpern, J. Reine Angew. Math., **209**, 1962, 54–71.
Leopoldt,H.-W. [75]: Eine p-adische Theorie der Zetawerte, II, J. Reine Angew. Math., **274/275**, 1975. 224–239.
Lepistö,T. [63]: The first factor of the class number of the cyclotomic field $k(\exp(2\pi i/p^n))$, Ann. Univ. Turku, AI, **70**, 1963, 1–7.
Lepistö,T. [66]: On the first factor of the class-number of the cyclotomic field and Dirichlet's L-functions, Ann. Acad. Sci. Fenn. Ser. A1, **387**, 1966, 1–53.
Lepistö,T. [67]: On the first factor of the class number of the cyclotomic field $k(\exp(2\pi i/p^u))$, Ann. Univ. Turku, AI, **108**, 1967, 1–8.
Lepistö,T. [68]: An upper bound for the first factor of the class number of the cyclotomic field $k(\exp\left(\frac{2\pi i}{p^u}\right))$, Ann. Univ. Turku, AI, **116**, 1968, 1–8.
Lepistö,T. [69]: On the class number of the cyclotomic field $k(\exp(2\pi i/p^n))$, Ann. Univ. Turku, AI, **125**, 1969, 1–13.
Lepistö,T. [70]: An estimate for the class number of the Abelian field, Ann. Acad. Sci. Fenn. Ser. A1, **473**, 1970, 1–15.
Lepistö,T. [74]: On the growth of the first factor of the prime cyclotomic field, Ann. Acad. Sci. Fenn. Ser. A1, **577**, 1974, 1–21.
Lequain,Y. [85]: A local characterization of Noetherian and Dedekind rings, Proc. Amer. Math. Soc., **94**, 1985, 369–370.
Lerch,M. [03]: Über die arithmetische Gleichung $Cl(-\Delta) = 1$, Math. Ann., **57**, 1903, 568–571.
Lerch,M. [05]: Essai sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers, Acta Math., **29**, 1905, 333–424; II, **30**, 1906, 203–294.
Letard,P. [95]: Valeur minimum des discriminants des corps de nombers de degré 9 totalement réels sous GRH, C.R. Acad. Sci. Paris, **320**, 1995, 135–138.
Lettl,G. [87]: Characterization of irreducible integers by their norms, Colloq. Math., **54**, 1987, 325–332.
Lettl,G. [90a]: The ring of integers of an abelian field, J. Reine Angew. Math., **404**, 1990, 162–170.
Lettl,G. [90b]: A note on Thaine's circular units, J. Number Theory, **35**, 1990, 224–226.
Lettl,G. [98]: Relative Galois module structure of integers of local abelian fields, Acta Arith., **85**, 1998, 235–248.
Leutbecher,A. [85]: Euclidean fields having a large Lenstra constant, Ann. Inst. Fourier, **35**, 1985, no.2, 83–106.
Leutbecher,A.,Martinet,J. [82a]: Lenstra's constant and Euclidean number fields, Astérisque, **94**, 1982, 87–131.
Leutbecher,A.,Martinet,J. [82b]: Constante de Lenstra et corps de nombres euclidiens, Sém. Théor. Nombres Bordeaux, 1981/82, exp.4.
Levesque,C. [81]: Systémes fondamentaux d'unités de certains composés de deux corps quadratiques, I, Canad. J. Math., **33**, 1981, 937–945.

Levesque,C. [82]: Systémes fondamentaux d'unités de certains corps de degré 4 et de degré 8 sur Q, Canad. J. Math., **34**, 1982, 1059–1090.

Levesque,C.,Lu,H.W. [96]: On S.Chowla's conjecture, Acta Math. Acad. Sci. Hungar., **70**, 1996, 237–246.

Levi,F. [31]: Zur Irreduzibilität der Kreisteilungspolynome, Compositio Math., **1**, 1931, 303–304.

Lewin,J. [67]: Subrings of finite index in finitely generated rings, J. Algebra, **5**, 1967, 84–88.

Lewis,D.J. [72]: Invariant sets of morphisms in projective and affine number spaces, J. Algebra, **20**, 1972, 419–434.

Lewis,D.J.,Mahler,K. [60]: On the representation of integers by binary forms, Acta Arith., **6**, 1960/61, 333–363.

Lewis,D.J.,Schinzel,A.,Zassenhaus,H. [66]: An extension of the theorem of Bauer and polynomials of certain special type, Acta Arith., **11**, 1966, 345–352.

Lewittes,J. [83]: Characters and decomposition of a representation in a number field, J. Number Theory, **16**, 1983, 31–48.

Li,H.-C. [96]: $\mathfrak{p}$-adic periodic points and Sen's theorem, J. Number Theory, **56**, 1996, 309–318.

Liang,J.J. [73]: On discriminants and maximal orders, Acta Math. Acad. Sci. Hungar., **24**, 1973, 41–57.

Liang,J.J. [76]: On the integral basis of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., **286/7**, 1976, 223–226.

Liang,J.J.,Mead,G.F.Jr. [83]: On matrix equations over the ring of p-adic integers, Comm. Algebra, **11**, 1983, 1237–1252.

Liang,J.,Zassenhaus,H. [69]: On a problem of Hasse, Math. Comp., **23**, 1969, 515–519.

Liang,J.,Zassenhaus,H. [77]: The minimum discriminant of sixth degree totally complex algebraic number fields, J. Number Theory, **9**, 1977, 16–35.

Liardet,P. [70]: Transformations rationnelles et ensembles algébriques, Thése 3 cycle, Marseille 1970.

Liardet,P. [71]: Sur les transformations polynomiales et rationnelles, Sém. Th. Nombres, Bordeaux, 1971/72, exp.29.

Liardet,P. [72]: Sur une conjecture de W.Narkiewicz, C.R. Acad. Sci. Paris, **274**, 1972, 1836–1838.

Liardet,P. [75]: Stabilité algébrique et topologies hilbertiennes, Sém. Delange–Pisot–Poitou, **17**, 1975/76, exp.8.

Lichtenbaum,S. [82]: Values of L-functions of Jacobi-sum Hecke characters of abelian fields, in: *Number Theory Related to Fermat's Last Theorem, Cambridge, Mass., 1981*, 207–218. Birkhäuser 1982.

Lidl,R.,Niederreiter,H. [83]: *Finite Fields*, Addison-Wesley 1983; 2nd edition: *Introduction to Finite Fields and their Applications*, Cambridge 1994.

Lienen,H.v. [78]: The quadratic form $x^2 - 2py^2$, J. Number Theory, **10**, 1978, 10–15.

Lind,D.A. [74]: Ergodic automorphisms of the infinite torus are Bernoulli, Israel J. Math., **17**, 1974, 162–168.

Lind,D.,Schmidt,K.,Ward,T. [90]: Mahler meaure and entropy for commuting automorphisms of compact groups, Invent. math., **101**, 1990, 593–629.

van der Linden,F.J. [84a]: *Euclidean Rings with Two Infinite Primes*, Thesis, Univ. Amsterdam 1984.

van der Linden,F.J. [84b]: Euclidean rings of integers of fourth degree fields, in: *Number Theory, Noordwijkerhout 1983*, 139–148, Lecture Notes in Math., **1068**, Springer 1984.

Linnik,J.V. [42]: On a conditional theorem of J.E.Littlewood, Dokl. Akad. Nauk SSSR, **37**, 1942, 142–144. (Russian)

Linnik,J.V. [43]: The "analogy property" of L-series and Siegel's theorem, Dokl. Akad. Nauk SSSR, **38**, 1943, 115–117. (Russian)
Linnik,J.V. [50]: An elementary proof of Siegel's theorem based on the method of I.M.Vinogradov, Izv. Akad. Nauk SSSR, Ser. Mat., **14**, 1950, 327–342. (Russian)
Linnik,J.V.,Vinogradov,A.I. [66]: Hyperelliptic curves and the smallest prime quadratic residue, Dokl. Akad. Nauk SSSR, **168**, 1966, 259–261. (Russian)
Lippman,R.A. [63]: Note on irregular discriminants, J. London Math. Soc., **38**, 1963, 385–386.
Littlewood,J.E. [28]: On the class-number of the corpus $P(\sqrt{-k})$, Proc. London Math. Soc., (2) **27**, 1928, 358–372.
Litver,E.L. [49]: On the number of ideal classes in certain special fields, Dokl. Akad. Nauk SSSR, **66**, 1949, 335–338. (Russian)
Litver,E.L. [55]: Fundamental basis of a composite of quadratic fields, Uchen. Zap. Univ. Rostov, **32**, 1955, 29–36 (Russian)
Llorente,P.,Nart,E. [83]: Effective determination of the decomposition of the rational primes in a cubic field, Proc. Amer. Math. Soc., **87**, 1983, 579–585.
Llorente,P.,Nart,E.,Vila,N. [84]: Discriminants of number fields defined by trinomials, Acta Arith., **43**, 1984, 368–373.
Llorente,P.,Quer,J. [88a]: On the 3-Sylow subgroup of the class group of quadratic fields, Math. Comp., **50**, 1988, 321–333.
Llorente,P.,Quer,J. [88b]: On totally real cubic fields with discriminant $D < 10^7$, Math. Comp., **50**, 1988, 581–594.
Lloyd–Smith,C.W. [84]: On a problem of Favard concerning algebraic integers, Bull. Austral. Math. Soc., **29**, 1984, 111–121.
Lloyd–Smith,C.W. [85a]: Algebraic numbers near the unit circle, Acta Arith., **45**, 1985, 43–57.
Lloyd–Smith,C.W. [85b]: On minimal diameters of algebraic integers in J-fields, J. Number Theory, **21**, 1985, 299–318.
Lochter,M. [93]: On equivalent number fields with special Galois groups, Israel J. Math., **84**, 1993, 89–96.
Lochter,M. [94a]: Weakly Kronecker equivalent number fields and global norms, Acta Arith., **67**, 1994, 105–121.
Lochter,M. [94b]: Weakly Kronecker equivalent number fields, Acta Arith., **67**, 1994, 295–312.
Lochter,M. [95]: New characterizations of Kronecker equivalence, J. Number Theory, **53**, 1995, 115–136.
Long,R. [71]: Steinitz classes of cyclic extensions of prime degree, J. Reine Angew. Math., **250**, 1971, 87–98.
Long,R. [72]: The module structure of some tamely ramified extensions of algebraic number fields, in: *Proceedings of the Number Theory Conference, Boulder*, 139–141, Boulder 1972.
Long,R. [75]: Steinitz classes of cyclic extensions of degree l^ν, Proc. Amer. Math. Soc., **49**, 1975, 297–304.
Long,R.L. [77]: *Algebraic Number Theory*, Marcel Dekker, 1977.
Lorenz,F. [80]: Über eine Verallgemeinerung des Hasseschen Normensatzes, Math. Z., **173**, 1980, 203–210.
Lorenz,F. [82]: Zur Theorie der Normenreste, J. Reine Angew. Math., **334**, 1982, 157–170.
Louboutin,R. [83]: Sur la mesure de Mahler d'un nombre algébrique, C.R. Acad. Sci. Paris, **296**, 1083, 707–708.
Louboutin,S. [88]: Continued fractions and real quadratic fields, J. Number Theory, **30**, 1988, 167–176.

Louboutin,S. [89]: Groupes de classes d'idéaux triviaux, Acta Arith., **54**, 1989, 61–74.
Louboutin,S. [90]: Prime producing quadratic polynomials and class-numbers of real quadratic fields, **42**, 1990, 315–341; corr. **42**, 1990, p.1131.
Louboutin,S. [91]: Extensions du théorème de Frobenius-Rabinowitsch, C.R. Acad. Sci. Paris, **312**, 1991, 711–714,
Louboutin,S. [92a]: Minoration au point 1 des fonctions L et détermination des corps sextiques abéliens totalement imaginaires principaux, Acta Arith., **62**, 1992, 109–124.
Louboutin,S. [92b]: Détermination des corps quartiques cycliques totalement imaginaires à groupe des classes d'idéaux d'exposant ≤ 2, Manuscripta Math., **77**, 1992, 385–404.
Louboutin,S. [93a]: Calcul des nombres de classes relatifs: application aux corps octiques quaternioniques à multiplication complexe, C.R. Acad. Sci. Paris, **317**, 1993, 643–646.
Louboutin,S. [93b]: Majorations explicites de $|L(1,\chi)|$, C.R. Acad. Sci. Paris, **316**, 1993, 11–14; II, **323**, 1996, 443–446; III, **332**, 2001, 95–98.
Louboutin,S. [94a]: On the class number one problem for non-normal quartic CM-fields, Tôhoku Math. J., (2) **46**, 1994, 1–12.
Louboutin,S. [94b]: The exponent 2-class-group problem for non-Galois over Q quartic fields that are quadratic extensions of imaginary quadratic fields, J. Number Theory, **49**, 1994, 133–141.
Louboutin,S. [94c]: Lower bounds for relative class numbers of CM-fields, Proc. Amer. Math. Soc., **120**, 1994, 425–434.
Louboutin,S. [95a]: Determination of all nonquadratic imaginary cyclic number fields of 2-power degrees with ideal class groups of exponent ≤ 2, Math. Comp., **64**, 1995, 323–340.
Louboutin,S. [95b]: Une remarque sur l'exposant du groupe des classes d'idéaux des corps cubiques, C.R. Acad. Sci. Paris, **320**, 1995, 1161–1163.
Louboutin,S. [96a]: Determination of all quaternion octic CM-fields with class number 2, J. London Math. Soc., (2) **54**, 1996, 227–238.
Louboutin,S. [96b]: A finiteness theorem for imaginary abelian fields, Manuscripta Math., **91**, 1996, 343–352.
Louboutin,S. [96c]: Class group problems for cubic number fields, Japan J. Math., **23**, 1997, 365–378.
Louboutin,S. [97a]: CM-fields with cyclic ideal class group of 2-power orders, J. Number Theory, **67**, 1997, 1–10.
Louboutin,S. [97b]: The class number one problem for the non-abelian normal CM-fields of degree 16, Acta Arith., **82**, 1997, 173–196.
Louboutin,S. [97c]: Powerful necessary conditions for class number problems, Math. Nachr., **183**, 1997, 173–184.
Louboutin,S. [98a]: Upper bounds for $|L(1,\chi)|$ and applications, Canad. J. Math., **50**, 1998, 794–815.
Louboutin,S. [98b]: Majorations explicites du résidu au point 1 des fonctions zêta de certains corps de nombres, J. Math. Soc. Japan, **50**, 1998, 57–69.
Louboutin,S. [98c]: The imaginary cyclic sextic fields with class numbers equal to their genus class numbers, Colloq. Math., **75**, 1998, 205–212.
Louboutin,S. [99a]: The class number one problem for the dihedral and dicyclic CM-fields, Colloq. Math., **80**, 1999, 259–265.
Louboutin,S. [99b]: The nonquadratic imaginary cyclic fields of 2-power degrees with class numbers equal to their genus class numbers, Proc. Amer. Math. Soc., **127**, 1999, 355–361.

Louboutin,S. [99c]: Class-group problems for cubic number fields, Japan J. Math., (N.S.) **23**, 1997. 265–278.
Louboutin,S. [00]: Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s = 1$ and relative class numbers, J. Number Theory, **85**, 2000, 263–282.
Louboutin,S. [01a]: Computation of $L(0, \chi)$ and of relative class numbers of CM-fields, Nagoya Math. J., **161**, 2001, 171–191.
Louboutin,S. [01b]: Class number and class group problems for some non-normal totally real cubic number fields, Manuscripta Math., **106**, 2001, 411–427.
Louboutin,S. [02a]: The exponent three class group problem for some real cyclic cubic number fields, Proc. Amer. Math. Soc., **130**, 2002, 353–361.
Louboutin,S. [02b]: Computation of class numbers of quadratic number fields, Math. Comp., **71**, 2002, 1735–1743.
Louboutin,S. [03]: Note on a hypothesis implying the non-vanishing of Dirichlet L-series $L(s, \chi)$ for $s > 0$ and real characters χ, Colloq. Math., **96**, 2003, 207–212.
Louboutin,S.,Mollin,R.A.,Williams,H.C. [92]: Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers, Canad. J. Math., **44**, 1992, 824–642.
Louboutin,S.,Mollin,R.A.,Williams,H.C. [93]: Class groups of exponent two in real quadratic fields, in: *Advances in Number Theory*, 499–513, Oxford 1993.
Louboutin,S.,Okazaki R. [94]: Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one, Acta Arith., **67**, 1994, 47–62.
Louboutin,S.,Okazaki R. [98]: The class number one problem for some non-Abelian normal CM-fields of 2-power degrees, Proc. London Math. Soc., (3) **76**, 1998, 523–548.
Louboutin,S.,Okazaki R. [99]: Determination of all quaternion CM-fields with ideal class group of exponent 2, Osaka Math. J., **36**, 1999, 229–257.
Louboutin,S.,Okazaki R. [03]: Exponents of the ideal class groups of the CM number fields, Math. Z., **243**, 2003, 155–159.
Louboutin,S. Okazaki R., Olivier,M. [97]: The class number one problem for some non-Abelian normal CM-fields, Trans. Amer. Math. Soc., **349**, 1997, 3657–3678.
Louboutin,S.,Park Y.-H. [00]: Class number problems for dicyclic CM-fields, Publ. Math. Debrecen, **57**, 2000, 283–295.
Low,M.E. [68]: Real zeros of the Dedekind zeta function of an imaginary quadratic field, Acta Arith., **14**, 1968, 117–140.
Loxton,J.H. [74a]: Products related to Gauss sums, J. Reine Angew. Math., **268/269**, 1974, 53–67.
Loxton,J.H. [74b]: On a cyclotomic diophantine equation, J. Reine Angew. Math., **270**, 1974, 164–168.
Loxton,J.H. [78]: Some conjectures concerning Gauss sums, J. Reine Angew. Math., **297**, 1978, 153–158.
Lu,H.W. [79]: On the class number of real quadratic fields, Sci. Sinica, 1979, Special Issue, II, 118–130.
Lubelski,S. [36]: Zur Gaussschen Kompositionstheorie der binären quadratischen Formen, J. Reine Angew. Math., **176**, 1936, 56–60.
Lubelski,S. [39]: Zur Arithmetisierung des Beweises des Minkowskischen Diskriminanten und Kronecker-Weberschen Einbettungssatzes, Acta Arith., **3**, 1939, 235–254.
Lubelski,S. [60]: Unpublished results in number theory: I. Quadratic forms in a Euclidean ring, Acta Arith., **6**, 1960/61, 217–224.
Lubin,J. [81]: The local Kronecker-Weber theorem, Trans. Amer. Math. Soc., **267**, 1981, 133–138.

Lundström,P. [01]: Normal integral bases for infinite abelian extensions, Acta Arith., **100**, 2001, 79–83.
Luthar,I.S. [66]: A generalization of a theorem of Landau, Acta Arith., **12**, 1966/67, 223–228.
Macaulay,F.S. [13]: On the resolution of a given modular system into primary systems including some properties of Hilbert numbers, Math. Ann., **74**, 1913, 66–121.
Macaulay,F.S. [16]: *The Algebraic Theory of Modular Systems*, Cambridge 1916.
MacCluer,C.R. [68]: A reduction of the Čebotarev density theorem to the cyclic case, Acta Arith., **15**, 1968, 45–47.
MacCluer,C.R. [71]: Non-principal divisors among the values of polynomials, Acta Arith., **19**, 1971, 319–320.
MacCluer,C.R.,Parry,C.J. [75]: Units of modulus 1, J. Number Theory, **7**, 1975, 371–375.
MacKenzie,R.,Scheunemann,J. [71]: A number field without a relative integral basis, Amer. Math. Monthly, **78**, 1971, 882–883.
MacKenzie,R.E.,Whaples,G. [56]: Artin-Schreier equations in characteristic zero, Amer. J. Math., **78**, 1956, 473–485.
MacLane,S. [36]: A construction for prime ideals as absolute values of an algebraic number field, Duke Math. J., **2**, 1936, 492–510.
Mac Lane,S. [39a]: Steinitz towers for modular fields, Trans. Amer. Math. Soc., **46**, 1939, 23–45.
Mac Lane,S. [39b]: Subfields and automorphisms groups of p-adic fields, Ann. of Math., (2) **40**, 1939, 23–45.
Madan,M.L. [70]: On class numbers of algebraic number fields, J. Number Theory, **2**, 1970, 116–119.
Madan,M.L. [72]: Class groups of global fields, J. Reine Angew. Math., **252**, 1972, 171–177.
Madden,D.J.,Vélez,W.Y. [80]: A note on the normality of unramified abelian extensions of quadratic extensions, Manuscripta Math., **30**, 1980, 235–240.
Magnus,W. [34]: Über den Beweis des Hauptidealsatzes, J. Reine Angew. Math., **170**, 1934, 235–240.
Mahler,K. [34]: On Hecke's theorem on the real zeros of the L-functions and the class number of quadratic fields, J. London Math. Soc., **9**, 1934, 298–302.
Mahler,K. [50]: On algebraic relations between two units in an algebraic field, in: *Algébre et Théorie des Nombres*, 47–55, CNRS 1950.
Mahler,K. [62]: On some inequalities for polynomials in several variables, J. London Math. Soc., **37**, 1962, 341–344.
Mahler,K. [64]: Inequalities for ideal bases in algebraic number fields, J. Austral. Math. Soc., **4**, 1964, 425–448.
Mahler,K. [73]: *Introduction to p-adic Numbers and their Functions*, Cambridge 1973.
Maillot,V. [00]: Géométrie d'Arakelov des variétés toriques et fibrés en droites intégrables, Mém. Soc. Math. France, **80**, Paris 2000.
Maire,C. [97]: Tours de Hilbert des extensions cubiques cycliques de Q, Manuscripta Math., **92**, 1997, 303–323.
Maire,C. [98]: Un raffinement du théorème de Golod-Safarevic, Nagoya Math. J., **150**, 1998, 1–11.
Maire,C. [00]: On infinite unramified extensions, Pacific J. Math., **192**, 2000, 135–142.
Mäki,S. [80]: *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., **797**, Springer 1980.

Mäki,S. [85]: On the density of Abelian number fields, Ann. Acad. Sci. Fenn. Ser. A1, **54**, 1985, 1–104.
Mäki,S. [88]: The conductor density of cyclic fields of square-free degree, Ann. Univ. Turku, AI, no.191, 1988, 1–31.
Mäki,S. [93]: The conductor density of abelian number fields, J. London Math. Soc., (2) **47**, 1993, 18–30.
Maknis,M. [75a]: On Hecke Z-functions of an imaginary quadratic field, Lit. Mat. Sb., **15**, 1975, no.1, 157–172. (Russian)
Maknis,M. [75b]: Zeros of Hecke Z-functions and the distribution of prime numbers of an imaginary quadratic field, Lit. Mat. Sb., **16**, 1976, no.1, 173–180. (Russian)
Maknis,M. [76]: Density theorems of Hecke Z-functions and the distribution of prime numbers of an imaginary quadratic field, Lit. Mat. Sb., **15**, 1975, no.1, 173–184. (Russian)
Maknis,M. [80]: The "large sieve" in quadratic fields, Lit. Mat. Sb., **20**, 1980, no.1, 173–180. (Russian)
Mallik,A. [81a]: New formulations of the class number one problem, Acta Arith., **39**, 1981, 361–364.
Mallik,A. [81b]: Bounding L-functions by class numbers, Acta Arith., **39**, 1981, 365–368.
Manin,Yu.I. [71]: Le groupe de Brauer-Grothendieck et géométrie diophantienne, in: *Proceedings of the ICM Nice*, **I**, 401–411, Paris 1971.
Man,S.H. [98]: A note on Dedekind domains, Rocky Mountain J. Math., **28**, 1998, 655–656.
Mann,H.B. [50]: On the field of origin of an ideal, Canad. J. Math., **2**, 1950, 16–21.
Mann,H.B. [54]: A generalization of a theorem of Ankeny and Rogers, Rend. Circ. Mat. Palermo, (2) **3**, 1954, 476–477.
Mann,H.B. [55]: *Introduction to Algebraic Number Theory*, Columbus 1955.
Mann,H.B. [58]: On integral bases, Proc. Amer. Math. Soc., **9**, 1958, 167–172.
Mann,H.B. [65]: On linear relations between roots of unity, Mathematika, **12**, 1965, 107–117.
Mann,H.B.,Vélez,W.Y. [76]: Prime ideal decomposition in $F(\sqrt[n]{\mu})$, Monatsh. Math., **81**, 1976, 131–139.
Mann,H.B.,Yamamoto,K. [67]: On canonical bases of ideals, J. Combin. Theory, **2**, 1967, 71–76.
Marcus,D.A. [77]: *Number Fields*, Springer 1977.
Marko,F. [96]: On the existence of p-units and Minkowski units in totally real cyclic fields, Abh. Math. Sem. Univ. Hamburg, **66**, 1996, 89–111.
Marszałek,R.,Narkiewicz,W. [04]: Finite polynomial orbits in quadratic rings, The Ramanujan J., to appear.
Martel,B. [74]: Sur l'anneau des entiers d'une extension biquadratique d'un corps 2-adique, C.R. Acad. Sci. Paris, **278**, 1974, 117–120.
Martinet,J. [69]: Sur l'arithmétique des extensions galoisiennes à groupe Galois diédral d'ordre $2p$, Ann. Inst. Fourier, **19**, 1969, no.1, 1–80.
Martinet,J. [71a]: Modules sur l'algébre du groupe quaternionien, Ann. Sci. École Norm. Sup., (4) **4**, 1971, 399–408.
Martinet,J. [71b]: Anneau des entiers d'une extension galoisienne considéré comme module sur l'algébre du groupe de Galois, Bull. Soc. Math. France, Mém. **25**, 1971, 123–126.
Martinet,J. [72]: Sur les extensions à groupe de Galois quaternionien, C.R. Acad. Sci. Paris, **274**, 1972, 933–935.
Martinet,J. [73]: Bases normales et constante de l'équation fonctionnelle des fonctions L d'Artin, Séminaire Bourbaki, **26**, 1973/74, exp.450.

Martinet,J. [77a]: Character theory and Artin L-functions, in: *Algebraic Number Fields*, 1–87, Academic Press 1977.
Martinet,J. [77b]: H_8, in: *Algebraic Number Fields*, 525–560, Academic Press 1977.
Martinet,J. [78]: Tours de corps de classes et estimations de discriminants, Invent. math., **44**, 1978, 65–73.
Martinet,J. [79a]: Sur le constante de Lenstra des corps de nombres, Sém. Théor. Nombres Bordeaux, 1979/80, exp. 17.
Martinet,J. [79b]: Petits discriminants, Ann. Inst. Fourier, **29**, 1979, no.1, 159–179.
Martinet,J. [82]: Petits discriminants des corps de nombres, in: *Journées Arithmétiques (Exeter 1980)*, 151–193, Cambridge 1982.
Martinet,J. [85]: Methodes géometriques dans la recherche des petits discriminants, Sém. Delange–Pisot–Poitou, 1983/84, Progr. Math., **59**, 147–179, Birkhäuser 1985.
Martinet,J.,Payan,J.J. [67]: Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne, J. Reine Angew. Math., **228**, 1967, 15–37.
Martinet,J.,Payan,J.J. [68]: Sur les bases d'entiers des extensions galoisiennes et non abéliennes de degré 6 des rationnels, J. Reine Angew. Math., **229**, 1968, 29–33.
Masley,J.M. [75]: Solution of the class number two problem for cyclotomic fields, Invent. math., **28**, 1975, 243–244.
Masley,J.M. [76]: Solution of small class numbers problems for cyclotomic fields, Compositio Math., **33**, 1976, 179–186.
Masley,J.M. [77]: Odlyzko bounds and class number problems, in: *Algebraic Number Fields*, 465–474, London 1977.
Masley,J.M. [78a]: Class number of real cyclic number fields with small conductor, Compositio Math., **37**, 1978, 297–319.
Masley,J.M. [78b]: On the first factor of the class number of prime cyclotomic fields, J. Number Theory, **10**, 1978, 273–290.
Masley,J.M. [79]: Where are the number fields with small class numbers? in: *Number Theory, Carbondale 1979*, 221–242, Lecture Notes in Math., **751**, Springer 1979.
Masley,J.M.,Montgomery,H.L. [76]: Cyclotomic fields with unique factorization, J. Reine Angew. Math., **286/287**, 1976, 248–256.
Massy,R.,Nguyen-Quang-Do,T. [75]: Extension galoisiennes non abéliennes de degré p^3 sur un corps $\mathfrak{P}$-adique, C.R. Acad. Sci. Paris, **280**, 1975, A1345–A1347.
Massy,R.,Sodaïgui,B. [97]: Steinitz classes and quaternionic extensions, Proyecciones, **16**, 1997, 1–13.
Masuda,K. [57]: Certain subgroups of the idèle group, Proc. Japan Acad. Sci., **33** 1957, 70–72.
Mathews,G.B. [93]: On the algebraic integers derived from an irreducible cubic equation, Proc. London Math. Soc., **24**, 1893, 327–336.
Matlis,E. [70]: The two-generator problem for ideals, Michigan J. Math., **17**, 1970, 157–265.
Matsumura,N. [77]: On the class field tower of an imaginary quadratic number field, Mem. Fac. Sci. Kyushu Univ., **31**, 1977, 165–171.
Matthews,C.R. [79]: Gauss sums and elliptic functions, I, Invent. math., **52**, 1979, 163–185; II, **53**, 1979, 23–52.
Matusita,K. [44]: Über ein bewertungstheoretisches Axiomensystem für die Dedekind-Noethersche Idealtheorie, Japan J. Math., **19**, 1944, 97–110.
Matveev,E.M. [91]: On the size of integral algebraic numbers, Mat. Zametki, **49**, 1991, 152–154. (Russian)
Matveev,E.M. [99]: On the successive minima of the extended logarithmic height of algebraic numbers,, Mat. Sb., **190**, 1999, 89–108. (Russian)

Mauclaire,J.L. [83]: Sommes de Gauss modulo p^{α}, Proc. Japan Acad. Sci., **59**, 1983, 109–112, 161–163.
Maurer,D. [73]: The trace-form of an algebraic number field, J. Number Theory, **5**, 1973, 379–384.
Maurer,D. [78a]: Invariants of the trace-form of a number field, Linear and Multilinear Algebra, **6**, 1978, 33–36.
Maurer,D. [78b]: A matrix criterion for normal integral bases, Illinois J. Math., **22**, 1978, 672–681.
Maurer,D. [79]: Arithmetic properties of the idèle discriminant, Pacific J. Math., **85**, 1979, 393–401.
Maus,E. [67]: Arithmetisch disjunkte Körper, J. Reine Angew. Math., **226**, 1967, 184–203.
Maus,E. [68]: Die gruppentheoretische Struktur der Verzweigungsgruppenreihen, J. Reine Angew. Math., **230**, 1968, 1–28.
Maus,E. [73]: Relationen in Verzweigungsgruppen, J. Reine Angew. Math., **258**, 1973, 23–50.
Mautner,F.I. [53]: On congruence characters, Monatsh. Math., **57**, 1953, 307–316.
May,W. [70]: Unit groups of infinite abelian extensions, Proc. Amer. Math. Soc., **25**, 1970, 680–683.
Mayer,J. [29]: Die absolut-kleinsten Diskriminanten der biquadratischen Zahlkörper, S.B. Akad. Wien, IIa, **138**, 1929, 733–742.
Maza,A.C. de la [02]: Bounds for the smallest norm in an ideal class, Math. Comp., **71**, 2002, 1745–1758.
Mazur,B. [93]: On the passage from local to global in number theory, Bull. Amer. Math. Soc., (N.S.) **29**, 1993, 14–50.
Mazur,B.,Wiles,A. [84]: Class fields of abelian extensions of Q, Invent. math., **76**, 1984, 179–330.
McAuley,M.J. [81]: Topics in J-fields and a diameter problem, Ph.D. thesis, Univ. of Adelaide 1981.
McCall,T.M.,Parry,C.J.,Ranalli,R.R. [97]: The 2-rank of the class group of imaginary bicyclic biquadratic fields, Canad. J. Math., **49**, 1997, 283–300.
McCoy,D.C.,Parry,C.J. [90]: Lengths of irreducible factorizations in fields with small class number, Colloq. Math., **59**, 1990, 9–24.
McCoy,D.C.,Parry,C.J. [01]: Bicyclic biquadratic fields which contain irreducible rational primes, Indian J. Pure Appl. Math., **32**, 2001, 589–612.
McCulloh,L.R. [63]: Integral bases in Kummer extensions of Dedekind fields, Canad. J. Math., **15**, 1963, 755–765.
McCulloh,L.R. [66]: Cyclic extensions without relative integral bases, Proc. Amer. Math. Soc., **17**, 1966, 1191–1194.
McCulloh,L.R. [71]: Frobenius groups and integral bases, J. Reine Angew. Math., **248**, 1971, 123–126.
McCulloh,L.R. [77]: A Stickelberger condition on Galois module structure for Kummer extension of prime degree, in: *Algebraic Number Fields*, 561–588, London 1977.
McCulloh,L.R. [82]: Stickelberger relations in class groups and Galois module structure, in: *Journées Arithmétiques 1980*, 194–201, Cambridge 1982.
McCulloh,L.R. [83]: Galois module structure of elementary abelian extensions, J. Algebra, **92**, 1983, 102–134.
McCulloh,L.R, [87]: Galois module structure in abelian extensions, J. Reine Angew. Math., **375/376**, 1987, 259–306.
McDuffee,C.C. [31]: A method for determining the canonical basis of an ideal, Math. Ann., **105**, 1931, 663–665.

McEliece,R.J. [87]: *Finite Fields for Computer Scientists and Engineers*, Kluwer 1987.

McFeat,R.B. [71]: Geometry of numbers in adele spaces, Dissert. Math., **88**, 1971, 1–49.

McGettrick,A.D. [72]: On the biquadratic Gauss sum, Proc. Cambridge Philos. Soc., **71**, 1972, 79–83.

McQuillan,D.L. [62]: A generalization of a theorem of Hecke, Amer. J. Math., **84**, 1962, 306–316.

Mead,D.G.,Narkiewicz,W. [82]: The capacity of C_5 and free sets in C_m^2, Proc. Amer. Math. Soc., **84**, 1982, 308–310.

Mertens,F. [74]: Ueber einige asymptotische Gesetze der Zahlentheorie, J. Reine Angew. Math., **77**, 1874, 289–338.

Mertens,F. [94]: Über die Fundamentalgleichung eines Gattungsbereiches algebraischen Zahlen, SBer. Kais. Akad. Wissensch. Wien, **103**, 1894, 5–40.

Mertens,F. [05]: Ein Beweis des Satzes, dass jede Klasse von ganzzahligen primitiven binären quadratischen Formen des Hauptgeschlechts durch Duplikation entsteht, J. Reine Angew. Math., **129**, 1905, 181–186.

Mertens,F. [06]: Über zyklische Gleichungen, J. Reine Angew. Math., **131**, 1906, 87–112.

Mestre,J.F. [81]: Corps euclidiens, unités exceptionnelles et courbes elliptiques, J. Number Theory, **13**, 1981, 123–137.

Mestre,J.F. [85]: Courbes de Weil de conducteur 5077, C.R. Acad. Sci. Paris. **300**, 1985, 509–512.

Mestre,J.F. [92]: Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3, C.R. Acad. Sci. Paris, **315**, 1992, 371–374.

Metsänkylä,T. [67a]: Bemerkungen über den ersten Faktor der Klassenzahl des Kreiskörpers, Ann. Univ. Turku, AI, **105**, 1967, 1–15.

Metsänkylä,T. [67b]: Über den ersten Faktor der Klassenzahl des Kreiskörpers, Ann. Acad. Sci. Fenn. Ser. A1, **416**, 1967, 1–48.

Metsänkylä,T. [68a]: Über die Teilbarkeit der Relativklassenzahl des Kreiskörpers durch Zwei, Ann. Univ. Turku, AI, **118**, 1968, 1–8.

Metsänkylä,T. [68b]: Über die Teilbarkeit des ersten Faktors der Klassenzahl des Kreiskörpers, Ann. Univ. Turku, AI, **124**, 1968, 1–6.

Metsänkylä,T. [69]: Congruences modulo 2 for class number factors in cyclotomic fields, Ann. Acad. Sci. Fenn. Ser. A1, **453**, 1969, 1–12.

Metsänkylä,T. [70a]: A congruence for the class number of a cyclic field, Ann. Acad. Sci. Fenn. Ser. A1, **472**, 1970, 1–11.

Metsänkylä,T. [70b]: Estimations for L-functions and the class number of certain imaginary cyclic fields, Ann. Univ. Turku, AI, **140**, 1970, 1–11.

Metsänkylä,T. [71]: On prime factors of the relative class number of cyclotomic fields, Ann. Univ. Turku, AI, **149**, 1971, 1–8.

Metsänkylä,T. [72]: On the growth of the first factor of the cyclotomic class number, Ann. Univ. Turku, AI, **155**, 1972, 1–12.

Metsänkylä,T. [73]: A class number congruence for cyclotomic fields and their subfields, Acta Arith., **23**, 1973, 107–116.

Metsänkylä,T. [74]: Class numbers and μ-invariants of cyclotomic field, Proc. Amer. Math. Soc., **43**, 1974, 299–300.

Metsänkylä,T. [75a]: On the cyclotomic invariants of Iwasawa, Math. Scand., **37**, 1975, 61–75.

Metsänkylä,T. [75b]: On the Iwasawa invariants of imaginary abelian fields, Ann. Acad. Sci. Fenn. Ser. A1, **1**, 1975, no.2, 343–353.

Metsänkylä,T. [77]: A short proof for the nonvanishing of a character sum, J. Number Theory, **9**, 1977, 507–509.

Metsänkylä,T. [78]: Iwasawa invariants and Kummer congruences, J. Number Theory, **10**, 1978, 510–522.
Metsänkylä,T. [83]: An upper bound for the λ-invariant of imaginary abelian fields, Math. Ann., **264**, 1983, 5–8.
Metsänkylä,T. [84]: Maillet's matrix and irregular primes, Ann. Univ. Turku, AI, **186**, 1984, 72–79.
Metsänkylä,T. [97]: Letter to the editor, J. Number Theory, **64**, 1997, p.163.
Meyer,C. [57]: *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag 1957.
Meyer,C. [67]: Über die Bildung von elementar-arithmetischen Klasseninvarianten in reell-quadratischen Zahlkörpern mit der Klassenzahl Eins, in: *Algebraische Zahlentheorie, Oberwolfach 1964*, 162–215, Mannheim 1967.
Meyer,C. [70]: Bemerkungen zum Satz von Heegner-Stark über die imaginär-quadratischen Zahlkörper mit der Klassenzahl Eins, J. Reine Angew. Math., **242**, 1970, 179–214.
Meyer,C. [75]: Imaginäre bizyklische biquadratische Zahlkörper als Klassenkörper, Symposia Math., **15**, 1975, 365–387.
Meyer,W.,Perlis,R. [79]: On the genus of norm forms, Math. Ann., **246**, 1979/80, 117–119.
Meyer,Y. [70]: *Nombres de Pisot, nombres de Salem et analyse harmonique*, Lecture Notes in Math., **117**, Springer 1970.
Miki,H. [76]: On some Galois cohomology groups of a local field and its application to the maximal p-extension, J. Math. Soc. Japan, **28**, 1976, 114–122.
Miki,H. [77]: A note on Maus' ramification theorem, Tôhoku Math. J., (2) **29**, 1977, 61–68.
Miki,H. [78]: On Grunwald-Hasse-Wang theorem, J. Math. Soc. Japan, **30**, 1978, 313–325.
Miki,H. [94]: On the conductor of the Jacobi sum Hecke character, Compositio Math., **92**, 1994, 23–41.
Mills,W.H. [63]: Characters with preassigned values, Canad. J. Math., **15**, 1963, 169–171.
Milnor,J. [71]: *Introduction to Algebraic K-theory*, Princeton 1971.
Mines,R.,Richman,F. [81]: Dedekind domains, in: *Constructive Mathematics*, Lecture Notes in Math., **873**, 16–30, Springer 1981.
Mines,R.,Richman,F. [84]: Valuation theory: a constructive view, J. Number Theory, **19**, 1984, 40–62.
Minkowski,H. [91a]: Über die positiven quadratischen Formen und über kettenbruchähnlichen Algorithmen, J. Reine Angew. Math., **197**, 1891, 278–297 = *Gesammelte Abhandlungen*, **I**, 244–260, Leipzig-Berlin 1911.
Minkowski,H. [91b]: Théorèmes arithmétiques, J. Reine Angew. Math., **112**, 1891, 209–212 = *Gesammelte Abhandlungen*, **I**, 261–263, Leipzig-Berlin 1911.
Minkowski,H. [96a]: *Geometrie der Zahlen*, Leipzig 1896. [Reprint: Johnson 1968.]
Minkowski,H. [96b]: Zur Theorie der Kettenbrüche, Ann. Sci. École Norm. Sup., (2) **13**, 1896, 41–60 = *Gesammelte Abhandlungen*, **I**, 278–292, Leipzig-Berlin 1911.
Minkowski,H. [00]: Zur Theorie der Einheiten in den algebraischen Zahlkörpern, Nachr. Ges. Wiss. Göttingen, 1900, 90–93 = *Gesammelte Abhandlungen*, **I**, 316–319, Leipzig-Berlin 1911.
Minkowski,H. [07]: *Diophantische Approximationen*, Leipzig 1907. [Reprints: Chelsea 1957; Physica Verlag 1961.]
Mirimanoff,D. [91]: Sur une question de la théorie des nombres, J. Reine Angew. Math., **99**, 1891, 82–88.
Mishou,H. [01]: The universality theorem for L-functions associated with ideal class characters, Acta Arith., **98**, 2001, 395–401.

Mishou,H. [03]: The universality theorem for Hecke L-functions, Acta Arith., **110**, 2003, 45–71.
Mitchell,H.H. [26]: On classes of ideals in a quadratic field, Ann. of Math., (2) **27**, 1926, 297–314.
Mitsui,T. [56]: Generalized prime number theorem, Japan J. Math., **26**, 1956, 1–42.
Mitsui,T. [68]: On the prime ideal theorem, J. Math. Soc. Japan, **20**, 1968, 233–247.
Miyada,I. [95]: On imaginary abelian number fields of type $(2, 2, \ldots, 2)$ with one class in each genus, Manuscripta Math., **88**, 1995, 535–540.
Miyake,K. [80a]: On the general principal ideal theorem, Proc. Japan Acad. Sci., **56**, 1980, 171–174.
Miyake,K. [80b]: On the structure of the idèle group of an algebraic number field, Nagoya Math. J., **80**, 1980, 117–127; II, Tôhoku Math. J., (2) **34**, 1982, 101–112.
Miyake,K. [82]: On the units of an algebraic number field, J. Math. Soc. Japan, **34**, 1982, 101–112.
Miyake,K. [89]: Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem and the capitulation problem, Exposition Math., **7**, 1989, 289–346.
Miyata,T. [80]: A normal integral basis theorem for dihedral groups, Tôhoku Math. J., (2) **32**, 1980, 49–62.
Miyata,Y. [74]: On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field, Nagoya Math. J., **54**, 1974, 53–59.
Miyata,Y. [79]: On the module structure in a cyclic extension over a $\mathfrak{p}$-adic number field, Nagoya Math. J., **73**, 1979, 61–68.
Miyata,Y. [80]: On the module structure of a p-extension of a $\mathfrak{p}$-adic number field, Nagoya Math. J., **77**, 1980, 13–23.
Miyata,Y. [95]: On the Galois module structure of ideals and rings of all integers of $\mathfrak{p}$-adic number fields, J. Algebra, **177**, 1995, 627–646.
Moine,J.M. [72]: Quelques problèmes concernant les classes ambiges des corps quadratiques, Ann. Univ. Besançon, 1972, no.4, 1–63.
Möller,H. [76a]: Imaginär-quadratische Zahlkörper mit einklassigen Geschlechtern, Acta Arith., **30**, 1976, 179–186.
Möller,H. [76b]: Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahlkörper, J. Reine Angew. Math., **285**, 1976, 100–113.
Mollin,R.A. [83]: Class numbers and a generalized Fermat theorem, J. Number Theory, **16**, 1983, 420–429.
Mollin,R.A. [87]: Class number one criteria for real quadratic fields, I, Proc. Japan Acad. Sci., **63**, 1987, 121–125; II, 162–164.
Mollin,R.A. [88]: Necessary and sufficient condition for the class number of a real quadratic field to be one, and a conjecture of S.Chowla, Proc. Amer. Math. Soc., **102**, 1988, 17–21.
Mollin,R.A. [90]: On the divisor function and class-numbers of real quadratic fields, I, II, Proc. Japan Acad. Sci., **66**, 1990, 109–111, 274–277; IV, **68**, 1992, 15–17.
Mollin,R.A. [96a]: Quadratic polynomials producing consecutive distinct primes and class groups of complex quadratic fields, Acta Arith., **74**, 1996, 17–30.
Mollin,R.A. [96b]: An elementary proof of the Rabinowitsch-Mollin-Williams criterion for real quadratic fields, J. Math. Sci. (Calcutta), **7**, 1996, 17–27.
Mollin,R.A. [96c]: A completely general Rabinowitsch criterion for complex quadratic fields, Canad. Math. Bull., **39**, 1996, 106–110.
Mollin,R.A. [96d]: *Quadratics*, CRC Press 1996.
Mollin,R.A. [97]: Polynomials of quadratic type producing strings of primes, Canad. Math. Bull., **40**, 1997, 214–220.
Mollin,R.A. [98a]: Quadratic prime-producing polynomials, J.Math. Sci. (Calcutta), **9**, 1998, 1–8.

Mollin,R.A. [98b]: Class number one and prime-producing quadratic polynomials, Canad. Math. Bull., **41**, 1998, 328–334.
Mollin,R.A. [98c]: Richaud-Degert prime producers, Utilitas Math., **54**, 1998, 273–286.
Mollin,R.A. [99]: *Algebraic Number Theory*, Chapman & Hall 1999.
Mollin,R.A. [01]: Continued fractions and class number two, J.Math. Math. Sci., **27**, 2001, 565–571.
Mollin,R.A.,Williams.H.C. [88a]: A conjecture of S. Chowla via the generalized Riemann hypothesis, Proc. Amer. Math. Soc., **102**, 1988, 794–796; corr. **123**, 1995, p.975.
Mollin,R.A.,Williams.H.C. [88b]: On prime valued polynomials and class numbers of real quadratic fields, Nagoya Math. J., **112**, 1988, 143–151.
Mollin,R.A.,Williams.H.C. [89a]: Period four and real quadratic fields of class number one, Proc. Japan Acad. Sci., **65**, 1989, 89–93.
Mollin,R.A.,Williams.H.C. [89b]: Class number one for real quadratic fields, continued fractions and reduced ideals, in: *Number Theory and Applications*, 481–496, Kluwer 1989.
Mollin,R.A.,Williams.H.C. [90]: Continued fractions of period five and real quadratic fields of class number one, Acta Arith., **56**, 1990, 55–63.
Mollin,R.A.,Williams.H.C. [91a]: On a determination of real quadratic fields of class number one and related continued fraction period length less than 25, Proc. Japan Acad. Sci., **67**, 1991, 20–25.
Mollin,R.A.,Williams.H.C. [91b]: On the divisor function and class-numbers of real quadratic fields, III, Proc. Japan Acad. Sci., **67**, 1991, 338–342.
Mollin,R.A.,Williams.H.C. [92]: On real quadratic fields of class number two, Math. Comp., **59**, 1992, 625–632.
Mollin,R.A.,Zhang,L.C.,Kemp.P. [94]: A lower bound for the class number of a real quadratic field of ERD type, Canad. Math. Bull., **37**, 1994, 90–96.
Monsky,P. [83]: p-ranks of class groups in Z_p^d-extensions. Math. Ann., **263**, 1983, 509–514.
Montes,J.,Nart,E. [92]: On a theorem of Ore, J. Algebra, **146**, 1992, 318–334.
Montgomery,H.L. [77]: Extreme values of the Riemann zeta function, Comment. Math. Helv., **52**, 1977, 511–518.
Montgomery,H.L.,Rohrlich,D.E. [82]: On the L-functions of canonical Hecke characters of imaginary quadratic fields, II, Duke Math. J., **49**, 1982, 937–942.
Montgomery,H.L.,Vaughan,R.C. [99]: Extreme values of Dirichlet L-functions at 1, in: *Number Theory in Progress*, **II**, 1039–1052, de Gruyter 1999.
Montgomery,H.L.,Weinberger,P.J. [74]: Notes on small class numbers, Acta Arith., **24**, 1974, 529–542.
Montgomery,H.L.,Weinberger,P.J. [77]: Real quadratic fields with large class numbers, Math. Ann., **225**, 1977, 173–176.
Montouchet,M.N. [71]: Sur le nombre de classes de sous-corps cyclique de $Q^{(p)}$, $p \equiv 1 \pmod 3$, Proc. Japan Acad. Sci., **47**, 1971, 585–586.
Moore,M.E. [75]: A strong complement property of Dedekind domains, Czechoslov. Math. J., **25**, 1975, 282–283.
Mordell,L.J. [18]: The class number for definite binary quadratics, Messenger of Math., **47**, 1918, 138–142.
Mordell,L.J. [22a]: On the reciprocity formula for the Gauss's sums in the quadratic field, Proc. London Math. Soc., (2) **20**, 1922, 289–296.
Mordell,L.J. [22b]: On trigonometric series involving algebraic numbers, Proc. London Math. Soc., (2), **21**, 1922, 493–496.

Mordell,L.J. [31]: On Hecke's modular functions, zeta functions, and some other analytic functions in the theory of numbers, Proc. London Math. Soc., (2) **32**, 1931, 501–556.
Mordell,L.J. [34]: On the Riemann hypothesis and imaginary quadratic fields with a given class number, J. London Math. Soc., **9**, 1934, 289–298.
Mordell,L.J. [53]: On the linear independence of algebraic numbers, Pacific J. Math., **3**, 1953, 625–630.
Mordell,L.J. [60a]: On a Pellian equation conjecture, Acta Arith., **6**, 1960, 137–144; II, J. London Math. Soc., **36**, 1961, 282–288.
Mordell,L.J. [60b]: On recurrence formulae for the number of classes of definite binary quadratic forms, J. Indian Math. Soc., **24**, 1960, 367–378.
Mordell,L.J. [61]: The congruence $[\frac{1}{2}(p-1)]! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly, **68**, 1961, 145–146.
Mordell,L.J. [62]: On a cyclotomic resolvent, Archiv Math., **13**, 1962, 486–487.
Mordell,L.J. [63]: On a cyclotomic diophantine equation, J. math. pures appl., (9) **42**, 1963, 205–208.
Mordell,L.J. [64]: On Lerch's class number formulae for binary quadratic forms, Ark. Mat., **5**, 1964, 97–100.
Mordell,L.J. [65]: On the conjecture for the rational points on a cubic surface, J. London Math. Soc., **40**, 1965, 149–158.
Mordell,L.J. [69]: A norm ideal bound for a class of biquadratic fields, Norske Vid. Selsk. Forh., **42**, 1969, 53–55.
Mori,S. [40]: Allgemeine Z.P.I.-Ringe, J. Sci. Hiroshima Univ., A**10**, 1940, 117–136.
Morikawa,R. [68]: On the unit group of an absolutely cyclic number field of degree five, J. Math. Soc. Japan, **20**, 1968, 263–265.
Morikawa,R. [74]: On units of certain cubic number field, Abh. Math. Sem. Univ. Hamburg, **42**, 1974, 72–77.
Morishima,T. [33]: Über die Einheiten und Idealklassen des Galoischen Zahlkörpers und die Theorie der Kreiskörper der l^ν-ten Einheitswurzeln, Japan J. Math., **10**, 1933, 83–126.
Morishima,T. [34]: Über die Theorie der Kreiskörper der l^ν-ten Einheitswurzeln, Japan J. Math., **11**, 1934, 225–240.
Morishima,T. [66]: On the second factor of the class-number of the cyclotomic field, J. Math. Anal. Appl., **15**, 1966, 141–153.
Moriya,M. [30]: Ueber die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad, Proc. Imp. Acad. Tokyo, **6**, 1930, 245–247; Japan J. Math., **10**, 1933, 1–18.
Moriya,M. [34]: Über die Konstruktion algebraischer Zahlkörper unendliches Grades, J.Fac. Sci. Hokkaido Univ., **2**, 1934, 119–128.
Moriya,M. [50]: Rein arithmetischer Beweis über die Unendlichkeit der Primideale 1 Grades aus einem endlichen algebraischen Zahlkörper, J. Fac. Sci. Hokkaido Univ., **11**, 1950, 164–166.
Moroz,B.Z. [82]: Scalar products of L-functions with grössencharacters: its meromorphic continuation and natural boundary, J. Reine Angew. Math., **332**, 1982, 99–117.
Moroz,B.Z. [86]: *Analytic Arithmetic in Algebraic Number Fields*, Lecture Notes in Math., **1205**, Springer 1986.
Moroz,B.Z. [88]: On a class of Dirichlet series associated to the ring of representations of a Weil group, Proc. London Math. Soc., (3) **56**, 1988, 209–228.
Morton,P. [79]: On Rédei's theory of Pell equation, J. Reine Angew. Math., **307/8**, 1979, 373–398.
Morton,P. [82a]: Density results for the 2-classgroups and fundamental units of real quadratic fields, Studia Sci. Math. Hungar., **17**, 1982, 21–43.

Morton,P. [82b]: Density results for the 2-classgroups of imaginary quadratic fields, J. Reine Angew. Math., **323**, 1982, 156–187.
Morton,P. [83]: The quadratic number fields with cyclic 2-classgroups, Pacific J. Math., **108**, 1983, 165–175.
Morton,P. [90]: Governing fields for the 2-classgroup of $Q(\sqrt{-q_1q_2p})$ and a related reciprocity law, Acta Arith., **55**, 1990, 267–290.
Morton,P. [92]: Arithmetic properties of periodic points of quadratic maps, Acta Arith., **62**, 1992, 343–372; II, **87**, 1998, 89–102.
Morton,P.,Patel,P. [94]: The Galois theory of periodic points of polynomial maps, Proc. London Math. Soc., (3) **68**, 1994, 225–263.
Morton,P.,Silverman,J. [94]: Rational periodic points of rational functions, Internat. Math. Res. Notices, 1994, 97–110.
Morton,P.,Silverman,J. [95]: Periodic points, multiplicities and dynamical units, J. Reine Angew. Math., **461**, 1995, 81–122.
Moser,C. [81]: Nombre de classes d'une extension cyclique réelle de Q, de degré 4 ou 6 et de conducteur premier, Math. Nachr., **102**, 1981, 45–52.
Moser,C., Payan,J.J. [81]: Majoration du nombre de classes d'un corps cubique cyclique de conducteur premier, J. Math. Soc. Japan, **33**, 1981, 45–52.
Moser,N. [75]: Unités et nombre de classes d'une extension dièdrale de Q, Astérisque, **24/25**, 1975, 701–706.
Moser,N. [78]: *Contraintes galoisiennes sur le groupe des unités de certains extensions de Q – applications arithmétiques*, Thése, Grenoble 1978.
Moser,N. [79a]: Unités et nombre de classes d'une extension galosienne dièdrale de Q, Abh. Math. Sem. Univ. Hamburg, **48**, 1979, 54–75.
Moser,N. [79b]: Sur les unités d'une extension galoisienne non abélienne de degré pq du corps des rationnels, p et q nombres premiers impairs, Ann. Inst. Fourier, **29**, 1979, no.1, 137–158.
Moser,N. [83]: Théorème de densite de Tchebotareff et monogénéité de modules sur l'algébre d'un groupe métacyclique, Acta Arith., **42**, 1983, 311–323.
Mossinghoff,M.J. [98]: Polynomials with small Mahler measure, Math. Comp., **67**, 1998, 1697–1715.
Mostowski,A. [55]: Determination of the degree of certain algebraic numbers, Prace Mat., **1**, 1955, 239–252. (Polish)
Motoda,Y. [75]: On biquadratic fields, Mem. Fac. Sci. Kyushu Univ., **29**, 1975, 263–268.
Motoda,Y.,Nakahara,T.,Shah,S.I.A. [02]: On a problem of Hasse for certain imaginary Abelian fields, J. Number Theory, **96**, 2002, 326–334.
Motohashi,Y. [70]: A note on the mean value of the Dedekind zeta-function of the quadratic field, Math. Ann., **188**, 1970, 123–127.
Motzkin,Th. [45]: Sur l'équation irréducible $z^n + a_1z^{n-1} + \ldots + a_0 = 0$, $n > 1$, à coefficients complexes entiers, dont toutes les racines sont sur une droite. Les 11 classes de droites admissibles, C.R. Acad. Sci. Paris, **221**, 1945, 220–222.
Motzkin,Th. [47]: From among n conjugate algebraic integers $n-1$ can be approximatively given, Bull. Amer. Math. Soc., **53**, 1947, 159–163.
Motzkin,Th. [49]: The Euclidean algorithm, Bull. Amer. Math. Soc., **55**, 1949, 1142–1146.
Moussa,P.,Geronimo,J.S.,Bessis,D. [84]: Ensembles de Julia et propriétés de localization des familles itérées d'entiers algébriques, C.R. Acad. Sci. Paris, **299**, 1984, 281–284.
Mulholland,H.P. [60]: On the product of n complex homogeneous linear forms, J. London Math. Soc., **35**, 1960, 241–250.
Müller,W. [88]: On the distribution of ideals in cubic number fields, Monatsh. Math., **106**, 1988, 211–219.

Müller,W. [89a]: The mean square of the Dedekind zeta function in quadratic number fields, Math. Proc. Cambridge Philos. Soc., **106**, 1989, 403–417.
Müller,W. [89b]: On the asymptotic behaviour of the ideal counting function in quadratic number fields, Monatsh. Math., **108**, 1989, 301–323.
Müntz,C. [23]: Der Summensatz von Cauchy in beliebigen algebraischen Zahlkörpern und die Diskriminante derselben, Math. Ann., **90**, 1923, 279–291.
Müntz,C. [24]: Allgemeine Begründung der Theorie der höheren ζ-Funktionen, Abh. Math. Sem. Univ. Hamburg, **3**, 1924, 1–11.
Murty,M.Ram [83]: On Artin's conjecture, J. Number Theory, **16**, 1983, 147–168.
Murty,M.Ram [84]: An analogue of Artin's conjecture for abelian extensions, J. Number Theory, **18**, 1984, 241–148.
Murty,M.Ram [93]: A motivated introduction to the Langlands program, in: *Advances in Number Theory (Kingston, ON 1991)*, 37–66. Oxford University Press, 1993.
Murty,M.Ram [94]: Selberg's conjectures and Artin L-functions, Bull. Amer. Math. Soc., (N.S.) **31**, 1994, 1–14; II, in: *Current Trends in Mathematics and Physics*, 154–168, New Delhi 1995,
Murty,M.Ram [99]: Exponents of class groups of quadratic fields, in: *Topics in Number Theory, University Park PA 1997*, 229–239. Kluwer 1999.
Murty,M.Ram [02]: Recent developments in the Langlands program, CR Math. Rep. Acad. Sci. Canada, **24**, 2002, 33–54.
Murty,M.Ram,Murty,V.Kumar [87]: A variant of the Bombieri-Vinogradov theorem, in: *Number Theory (Montreal, 1985)*, 243–272, Amer. Math. Soc., 1987.
Murty,M.Ram,Petridis,Y.N. [01]: On Kummer's conjecture, J. Number Theory, **80**, 2001, 294–303.
Murty,V.Kumar [88]: Holomorphy of Artin L-functions, in: *Proceedings of the Ramanujan Centennial International Conference*, 55–66, Annamalainagar 1988.
Murty,V.Kumar [94]: The least prime which does not split completely, Forum Math., **6**, 1994, 555–565.
Murty,V.Kumar [00]: The least prime in a conjugacy class, C.R. Acad. Sci. Canada, **22**, 2000, 129–146.
Nagata,K. [86]: Artin's L-function and Gassmann equivalence, Tokyo J. Math., **9**, 1986, 357–364.
Nagata,M. [53]: On the theory of Henselian rings, Nagoya Math. J., **5**, 1953, 45–57; II, **7**, 1954, 1–19.
Nagata,M.,Nakayama,T.,Tuzuku,T. [53]: On an existence lemma in valuation theory, Nagoya Math. J., **6**, 1953, 59–61.
Nagell,T. [19]: Le discriminant de l'équation de la division du cercle, Norsk Mat. Tidsskr., **1**, 1919, 99–101.
Nagell,T. [22]: Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **1**, 1922, 140–150.
Nagell,T. [30]: Zur Theorie der kubischen Irrationalitäten, Acta Math., **55**, 1930, 33–65.
Nagell,T. [32]: Sätze über algebraische Ringe, Math. Z., **34**, 1932, 179–182.
Nagell,T. [38]: Bemerkung über die Klassenzahl reell-quadratischer Zahlkörper, Norske Vid. Selsk. Forh., **11**, 1938, 7–10.
Nagell,T. [39]: Bestimmung des Grades gewisser relativ-algebraischer Zahlen, Monatsh. Math. Phys., **48**, 1939, 61–74.
Nagell,T. [59]: Les points exceptionnels rationnels sur certain cubiques du premier genre, Acta Arith., **5**, 1959, 333–357.
Nagell,T. [60]: Les points exceptionnels sur les cubiques $ax^3 + by^3 + cz^3 = 0$, Acta Sci. Math. (Szeged), **21**, 1960, 173–180.

Nagell,T. [62]: Sur quelques questions dans la théorie des corps biquadratiques, Ark. Mat., **4**, 1962, 347–376.
Nagell,T. [64a]: Contributions à la théorie des corps et des pôlynomes cyclotomiques, Ark. Mat., **5**, 1964, 153–192.
Nagell,T. [64b]: Sur une propriété des unités d'un corps algébrique, Ark. Mat., **5**, 1964, 343–356.
Nagell,T. [65]: Contributions à la théorie des modules et des anneaux algébriques, Ark. Mat., **6**, 1965, 161–178.
Nagell,T. [66]: Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique, Ark. Mat., **6**, 1966, 269–289.
Nagell,T. [68a]: Sur les diviseurs premiers des polynômes, Acta Arith., **15**, 1968/69, 235–244.
Nagell [68b]: Quelques propriétés des nombres algébriques du quatrième degré, Ark. Mat., **7**, 1968, 517–525.
Nagell,T. [69a]: Quelques problèmes relatifs aux unités algébriques, Ark. Mat., **8**. 115–127.
Nagell,T. [69b]: Sur un type particulier d'unités algébriques, Ark. Mat., **8**, 1969, 163–184.
Naito,H. [95]: Dihedral extensions of degree 8 over the rational p-adic fields, Proc. Japan Acad. Sci., **71**, 1995, 17–18.
Nakagawa,J.,Horie,K. [88]: Elliptic curves with no rational points, Proc. Amer. Math. Soc., **104**, 1988, 20–24.
Nakagoshi,N. [75]: On indices of unit groups related to the genus number of Galois extensions, Sci. Rep. Kanazawa Univ., **20**, 1975, 7–13.
Nakagoshi,N. [79]: The structure of the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$, Nagoya Math. J., **73**, 1979, 41–60.
Nakagoshi,N. [81]: On the class number relations of abelian extension whose galois groups are of the type (p,p), Math. Rep. Toyama Univ., **4**, 1981, 91–106.
Nakagoshi,N. [84]: A note on l-class group of certain algebraic number fields, J. Number Theory, **19**, 1984, 140–147.
Nakahara,T. [70]: On the determination of fundamental units of certain real quadratic fields, Mem. Fac. Sci. Kyushu Univ., **24**, 1970, 300–304.
Nakahara,T. [73]: Examples of algebraic number fields which have not unramified extensions, Rep. Fac. Sci. Engrg. Saga Univ., **1**, 1973, 1–8.
Nakahara,T. [83]: On the indices and integral bases of noncyclic but Abelian biquadratic fields, Archiv Math., **41**, 1983, 504–508.
Nakahara,T. [87]: On the minimum index of a cyclic quartic field, Archiv Math., **48**, 1987, 322–325.
Nakahara,T. [93]: A simple proof for non-monogenesis of the rings of integers in some cyclic fields, in: *Advances in Number Theory, Kingston 1991*, 167–173. Clarendon Press 1993.
Nakamula,K. [79]: An explicit formula for the fundamental units of a real pure sextic number field and its Galois closure, Pacific J. Math., **83**, 1979, 463–471.
Nakamula,K. [82a]: A construction of the group of units of some number fields from certain subgroups, Tokyo J. Math., **5**, 1982, 85–106.
Nakamula,K. [82b]: Class number calculation of a cubic field from an elliptic unit, J. Reine Angew. Math., **331**, 1982, 114–123.
Nakamula,K. [85a]: Class number calculation of a quartic field from an elliptic unit, Acta Arith., **45**, 1985, 215–227.
Nakamula,K. [85b]: Class number calculation of a sextic field from an elliptic unit, Acta Arith., **45**, 1985, 229–247.
Nakamula,K. [89]: Elliptic units and the class numbers of non-Galois fields, J. Number Theory, **31**, 1989, 142–166.

Nakamula,K. [96]: Certain quartic fields with small regulators, J. Number Theory, **57**, 1996, 1–21.
Nakamura,Y. [59]: On the distribution of ideals with exactly r different prime divisors in an ideal class of an algebraic number field, Sci. Rep. Tokyo Kyoiku Daigaku, A **6**, 1959, 241–257.
Nakamura,Y. [74]: Degrees of Galois extensions and norms of prime ideals in algebraic number fields, Math. Japon., **19**, 1974, 135–138.
Nakano,N. [43]: Über die Umkehrbarkeit der Ideale in Integritätsbereichen, Proc. Imp. Acad. Tokyo, **19**, 1943, 230–234.
Nakano,S. [83a]: Class numbers of pure cubic fields, Proc. Japan Acad. Sci., **59**, 1983, 263–265.
Nakano,S. [83b]: On the construction of certain number fields, Tokyo J. Math., **6**, 1983, 389–395.
Nakano,S. [84]: On ideal class groups of algebraic number fields, Proc. Japan Acad. Sci., **60**, 1984, 74–77.
Nakano,S. [85]: On ideal class groups of algebraic number fields, J. Reine Angew. Math., **358**, 1985, 61–75.
Nakano,S. [86a]: Ideal class groups of cubic cyclic fields, Acta Arith., **46**, 1986, 297–300.
Nakano,S. [86b]: On the construction of pure number fields of odd degrees with large 2-class groups, Proc. Japan Acad. Sci., **62**, 1986, 61–64.
Nakano,S. [88]: Construction of pure cubic fields with large 2-class groups, Osaka Math. J., **25**, 1988, 161–170.
Nakatsuchi,S. [68]: A note on certain properties of algebraic number fields, Mem. Osaka Univ., **17**, 1968, 1–10.
Nakatsuchi,S. [70]: On a relation between Kronecker's assertion and Gassmann's theorem, Mem. Osaka Univ., **19**, 1970, 97–105.
Nakatsuchi,S. [72]: A note on regular domains of algebraic number fields, Mem. Osaka Univ., **21**, 1972, 205–211.
Nakatsuchi,S. [73]: A note on Kronecker's "Randwertsatz", J. Math. Kyoto Univ., **13**, 1973, 129–137.
Nakatsuchi,S. [75]: On Čebotarev-sets of normal number fields, Math. Japon., **20**, 1975, 183–206; suppl., **21**, 1976, 105–109.
Nakayama,T. [52]: Idéle-class factor sets and class field theory, Ann. of Math., (2) **55**, 1952, 73–84.
Narkiewicz,W. [62]: On polynomial transformations, Acta Arith., **7**, 1962, 241–249.
Narkiewicz,W. [64]: On algebraic number fields with non-unique factorization, Colloq. Math., **12**, 1964, 59–67; II, **15**, 1966, 49–58.
Narkiewicz,W. [66]: On natural numbers having unique factorization in a quadratic number field, Acta Arith., **12**, 1966, 1–22; II, **13**, 1967, 123–129.
Narkiewicz,W. [69]: On a theorem of A.Weil on derivations in number fields, Colloq. Math., **20**, 1969, 57–58.
Narkiewicz,W. [72]: Numbers with unique factorization in an algebraic number field, Acta Arith., **21**, 1972, 313–322.
Narkiewicz,W. [79]: Finite abelian groups and factorization problems, Colloq. Math., **42**, 1979, 319–330.
Narkiewicz,W. [80]: Normal order for a function associated with factorization into irreducibles, Acta Arith., **37**, 1980, 77–84.
Narkiewicz,W. [83]: *Number Theory*, World Scientific, 1983.
Narkiewicz,W. [86]: *Classical Problems in Number Theory*, Warszawa 1986.
Narkiewicz,W. [87]: A note on Artin's conjecture in algebraic number fields, J. Reine Angew. Math., **381**, 1987, 110–115.
Narkiewicz,W. [88]: Units in residue classes, Archiv Math., **51**, 1988, 238–241.

Narkiewicz,W. [89]: Polynomial cycles in algebraic number fields, Colloq. Math., **58**, 1989, 151–155.
Narkiewicz,W. [96]: Global class-field theory, in: *Handbook of Algebra*, **I**, 365–393, Elsevier 1996.
Narkiewicz,W. [00]: *The Development of Prime Number Theory*, Springer 2000.
Narkiewicz,W.,Pezda,T. [97]: Finite polynomial orbits in finitely generated domains, Monatsh. Math., **124**, 1997, 309–316.
Narkiewicz,W.,Schinzel,A. [69]: Ein einfacher Beweis des Dedekindschen Satzes über die Differente, Colloq. Math., **20**, 1969, 65–66.
Narkiewicz,W.,Śliwa,J. [78]: Normal order for certain functions associated with factorizations in number fields, Colloq. Math., **38**, 1978, 323–328.
Narkiewicz,W.,Śliwa,J. [82]: Finite abelian groups and factorization problems, II, Colloq. Math., **46**, 1982, 115–122.
Nart,E. [85]: On the index of a number field, Trans. Amer. Math. Soc., **289**, 1985, 171–183.
Nekovář,J. [92]: Kolyvagin's method for Chow groups of Koga-Sato varieties, Invent. math., **107**, 1992, 99–125.
Nemenzo,F.,Wada,H. [92]: An elementary proof of Gauss' genus theorem, Proc. Japan Acad. Sci., **68**, 1992, 94–95.
Netto,E. [83]: Notiz über Gleichungen, deren Discriminante ein Quadrat ist, J. Reine Angew. Math., **95**, 1883, 237–239.
Netto,E. [84]: Über die Factorenzerlegung der Discriminanten algebraischer Gleichungen, Math. Ann., **24**, 1884, 579–587.
Neubrand,M. [78]: Einheiten in algebraischen Funktionen- und Zahlkörpern, J. Reine Angew. Math., **303/304**, 1978, 170–204.
Neubrand,M. [81]: Scharen quadratischer Zahlkörper mit gleichgebauten Einheiten, Acta Arith., **39**, 1981, 125–132.
Neugebauer,A. [88]: On the zeros of the Dedekind zeta function near the real axis, Funct. Approx. Comment. Math., **16**, 1988, 165–167.
Neukirch,J. [67]: Zur Differententheorie, Archiv Math., **18**, 1967, 241–249.
Neukirch,J. [68]: Über eine algebraische Kennzeichnung der Henselkörper, J. Reine Angew. Math., **231**, 1968, 75–81.
Neukirch,J. [69a]: Kennzeichnung der p-adischen und der endlich-algebraischen Zahlkörper, Invent. math., **6**, 1969, 296–314.
Neukirch,J. [69b]: Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. Reine Angew. Math., **238**, 1969, 135–147.
Neukirch,J. [73]: Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. math., **21**, 1973, 59–116.
Neukirch,J. [74a]: Über die absolute Galoisgruppe algebraischer Zahlkörper, Jahresber. Deutsch. Math.-Verein., **76**, 1974, 18–37.
Neukirch,J. [74b]: Eine Bemerkung zum Existenzsatz von Grunwald-Hasse-Wang, J. Reine Angew. Math., **268/269**, 1974, 315–317.
Neukirch,J. [74c]: On an existence theorem of Grunwald's type, Bol. Soc. Brasil. Mat., **5**, 1974, 79–83.
Neukirch,J. [77]: Über die absoluten Galoisgruppen algebraischer Zahlkörper, Astérisque, **41/42**, 1977, 67–79.
Neukirch,J. [84]: Neubegründung der Klassenkörpertheorie, Math. Zeitschr., **186**, 1984, 557–574.
Neukirch,J. [86]: *Class Field Theory*, Springer 1986.
Neukirch,J. [92]: *Algebraische Zahlentheorie*, Springer 1992. [English translation: Springer 1999.]

Neukirch,J. [94]: Micro primes, Math. Ann., **298**, 1994, 629-666.
Neukirch,J.,Wingberg,K. [00]: *Cohomology of Number Fields*, Springer 2000.
v.Neumann,J. [26]: Zur Prüferschen Theorie der idealen Zahlen, Acta Sci. Math. (Szeged), **2**, 1926, 193–227.
Neumann,O. [73]: Relativ-quadratische Zahlkörper, deren Klassenzahlen durch 3 teilbar sind, Math. Nachr., **56**, 1973, 281–306.
Neumann,O. [77]: On maximal p-extensions, class numbers and unit signatures, Astérisque, **41/42**, 1977, 239–246.
Neumann,O. [81a]: Über die Anstösse zu Kummers Schöpfung der "idealen complexen Zahlen", in: *Mathematical Perspectives*, 179–199, Academic Press 1981.
Neumann,O. [81b]: Two proofs of the Kronecker-Weber theorem "according to Kronecker and Weber", J. Reine Angew. Math., **323**, 1981, 105–126.
Newman,M. [56]: Bounds for class numbers, Proc. Symposia Pure Math., **8**, 1965, 70–77.
Newman,M. [71]: Units in cyclotomic fields, J. Reine Angew. Math., **250**, 1971, 3–11.
Newman,M. [74a]: Diophantine equations in cyclotomic fields, J. Reine Angew. Math., **265**, 1974, 84–89; corr. **280**, 1976, 211–212.
Newman,M. [74b]: Units in arithmetic progression in an algebraic number field, Proc. Amer. Math. Soc., **43**, 1976, 266–268.
Newman,M. [90]: Consecutive units, Proc. Amer. Math. Soc., **108**, 1990, 303–306.
Newman,M. [93]: Units differing by rationals in a cyclotomic field, Linear and Multilinear Algebra, **34**, 1993, 55–57.
Newman,M.,Taussky,O. [58]: On a generalization of the normal basis in abelian algebraic number fields, Comm. Pure Appl. Math., **9**, 1958, 85–91.
Nicolae,F. [00]: Über die lineare Unabhängigkeit der Dedekindschen Zetafunktionen galoischer Zahlkörper, Math. Nachr., **220**, 2000, 111–113.
Niklasch,G. [94]: On the verification of Clark's example of a Euclidean but not norm-Euclidean number field, Manuscripta Math., **83**, 1994, 443–446.
Niklasch,G. [97]: Counting exceptional units, Collect. Math., **48**, 1997, 195–207.
Niklasch,G.,Smart,N.P. [98]: Exceptional units in a family of quartic fields, Math. Comp., **67**, 1998, 759–772.
Nishizawa,K.,Sekiguchi,K.,Yoshino,K. [91]: Location of algebraic integers and related topics, in: *Dynamical Systems and Related Topics*, 422–450, World Scientific, 1991.
Nóbrega,T. [90]: Circular units of an abelian number field, An. Acad. Brasil. Ciênc., **62**, 1990, 1–4.
Noether,E. [19]: Die arithmetische Theorie der algebraischen Funktionen einer Veränderlichen in ihrer Beziehung zu den übrigen Theorie und zu der Zahlkörpertheorie, Jahresber. Deutsch. Math.-Verein., **28**, 1919, 182–203.
Noether,E. [21]: Idealtheorie in Ringbereichen, Math. Ann., **83**, 1921, 24–66.
Noether,E. [27a]: Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann., **96**, 1926, 26–61.
Noether,E. [27b]: Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- oder Funktionenkörpers, J. Reine Angew. Math., **157**, 1927, 82–104.
Noether,E. [32]: Normalbasis bei Körpern ohne höhere Verzweigung, J. Reine Angew. Math., **167**, 1932, 147–152.
Noether,E. [33]: Der Hauptgeschlechtsatz für relativ-galoissche Zahlkörper, Math. Ann., **108**, 1933, 411–419.
Nordhoff,H.U. [74]: Explizite Darstellungen von Einheiten und ihre Anwendung auf Mehrklassigkeitsfragen bei reell-quadratischen Zahlkörpern, I, J. Reine Angew. Math., **268/9**, 1974, 131–149; II, **280**, 1976, 37–60.

Northcott,D.G. [55]: A note on classical ideal theory, Proc. Cambridge Philos. Soc., **51**, 1955, 766–767.
Notari,C. [78]: Sur le produit des conjugués à l'extérieur du cercle unité d'un nombre algébrique, C.R. Acad. Sci. Paris, **286**, 313–315.
Novikov,A.P. [62]: On class numbers of fields of complex multiplication, Izv. Akad. Nauk SSSR, Ser. Mat., **26**, 1962, 677–686. (Russian)
Novikov,A.P. [67]: On class numbers of fields which are abelian over an imaginary quadratic field, Izv. Akad. Nauk SSSR, Ser. Mat., **31**, 1967, 717–726. (Russian)
Novikov,A.P. [69]: On the regularity of prime divisors of first degree in an imaginary quadratic field, Izv. Akad. Nauk SSSR, Ser. Mat., **33**, 1969, 1059–1079. (Russian)
Novikov,A.P. [80]: Kronecker's limit formula in a real quadratic field, Izv. Akad. Nauk SSSR, Ser. Mat., **44**, 1980, 886–917. (Russian)
Nowak,W.G. [93]: On the distribution of integer ideals in algebraic number fields, Math. Nachr., **161**, 1993, 59–74.
Nymann,J. [67]: A Minkowskian type bound for a class of relative quadratic fields, Duke Math. J., **34**, 1967, 53–55.
Nyul,G. [01]: Power integral bases in mixed biquadratic number fields, Acta Acad. Paed. Agriensis, Sect. Math., **28**, 2001, 79–86.
Nyul,G. [02]: Non-monogeneity of multiquadratic number fields, Acta Math. Inf. Univ. Ostraviensis, **10**, 2002, 85–93.
Odlyzko,A. [75]: Some analytic estimates of class numbers and discriminants, Invent. math., **29**, 1975, 275–286.
Odlyzko,A. [76]: Lower bounds for discriminants of number fields, Acta Arith., **29**, 1976, 275–297; II, Tôhoku Math. J., (2) **29**, 1977, 209–216.
Odlyzko,A. [77]: On conductors and discriminants, in: *Algebraic Number Fields*, 377–407, Academic Press 1977.
Odlyzko,A. [90]: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions; a survey of recent results, Sém. Théor. Nombres Bordeaux, (2) **2**, 1990, 119–141.
Odlyzko,A.,Skinner,C.M. [93]: Nonexistence of Siegel zeros in towers of radical extensions, in: *A Tribute to Emil Grosswald: Number Theory and Related Analysis*, Contemp. Math., **143**, 1993, 499–511.
Odoni,R.W.K. [73a]: On Gauss sums mod p^n, Bull. London Math. Soc., **5**, 1973, 325–327.
Odoni,R.W.K. [73b]: The Farey density of norm subgroups of global fields, I, Mathematika, **20**, 1973, 155–169.
Odoni,R.W.K. [75a]: On the norms of algebraic integers, Mathematika, **22**, 1975, 71–80.
Odoni,R.W.K. [75b]: On norms of integers in a full module of an algebraic number field and the distribution of values of binary integral quadratic forms, Mathematika, **22**, 1975, 108–111.
Odoni,R.W.K. [76]: On a problem of Narkiewicz, J. Reine Angew. Math., **288**, 1976, 160–167.
Odoni,R.W.K. [77a]: Some global norm density results from an extended Čebotarev density theorem, in: *Algebraic Number Theory*, 485–495, London 1977.
Odoni,R.W.K. [77b]: A new equidistribution property of norms of ideals in given class, Acta Arith., **33**, 1977, 53–63.
Odoni,R.W.K. [78]: Representation of algebraic integers by binary quadratic forms and norm forms from full modules of extension fields, J. Number Theory, **10**, 1978, 324–333.
Odoni,R.W.K. [89]: On the distribution of norms of ideals in given ray-classes and the theory of central ray-class fields, Acta Arith., **52**, 1989, 373–397.

Odoni,R.W.K. [91a]: Weil numbers and CM-fields, II, J. Number Theory, **38**, 1991, 366–377.
Odoni,R.W.K. [91b]: On the number of integral ideals of given norm and ray-class, Mathematika, **38**, 1991, 185–190.
Oesterlé,J. [85]: Nombres de classes des corps quadratiques imaginaires, Sém. Bourbaki, vol. 1983/84, exp.631, Astérisque. **121/122**, 1985, 309–323.
Oesterlé,J. [88]: Le problème de Gauss sur le nombre de classes, Enseign. Math., (2) **34**, 1988,43–67.
Oh,J. [98]: On the λ-invariants of totally real fields, Proc. Japan Acad. Sci., **74**, 1998, 125–126.
Ohta,K. [72]: On the relative class number of a relative Galois number field, J. Math. Soc. Japan, **24**, 1972, 552–557.
Ohta,K. [78]: On the p-class group of a Galois number field and its subfields, J. Math. Soc. Japan, **30**, 1978, 763–770.
Ohta,K. [81]: On algebraic number fields whose class numbers are multiples of 3, Bull. Fac. Gen. Educ. Gifu Univ., 1981, 51–54.
Okada,T. [80]: Normal bases of class fields over Gauss's number field, J. London Math. Soc., (2) **22**, 1980, 221–225.
Okamoto,T. [76]: A remark on the relative class number of certain algebraic number fields, TRU Math., **12**, 1976, no.2, 1–3.
Okazaki,R. [91]: On evaluation of L-functions over real quadratic fields, J. Math. Kyoto Univ., **31**, 1991, 1125–1153.
Okazaki,R. [00]: Inclusion of CM-fields and divisibility of relative class numbers, Acta Arith., **92**, 2000, 319–338.
Okutsu,K. [82]: Integral basis of the field $Q(\sqrt[n]{a})$, Proc. Japan Acad. Sci., **58**, 1982, 219–222.
Olivier,M. [89]: Corps sextiques contenant un corps quadratique, I, Sém. Théor. Nombres Bordeaux, (2) **1**, 1989, 205–250; II, **2**, 1990, 49–102.
Olivier,M. [91a]: Corps sextiques contenant un corps cubique, III, Sém. Théor. Nombres Bordeaux, (2) **3**, 1991, 201–245.
Olivier,M. [91b]: Corps sextiques primitifs, IV, Sém. Théor. Nombres Bordeaux, (2) **2**, 1991, 381–404.
Olson,J.E. [69]: A combinatorial problem on finite Abelian groups, J. Number Theory, **1**, 1969, 8–10.
Omar,S. [00]: Majoration du premier zéro de la function zêta de Dedekind, Acta Arith., **95**, 2000, 61–65.
Omar,S. [01]: Localization of the first zero of the Dedekind zeta function, Math. Comp., **70**, 2001, 1607–1616.
O'Meara,O.T. [56]: Basis structure of modules, Proc. Amer. Math. Soc., **7**, 1956, 956–974.
O'Meara,O.T. [59]: Infinite dimensional quadratic forms over algebraic number fields, Proc. Amer. Math. Soc., **10**, 1959, 55–58.
O'Meara,O.T. [63]: *Introduction to Quadratic Forms*, Springer 1963.
O'Meara,O.T. [65]: On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math., **217**, 1965, 79–108.
Onabe,M. [76]: On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields, Natur. Sci. Rep. Ochanomizu Univ., **27**, 1976, 155–161.
Onabe,M. [78]: On idèle class groups of imaginary quadratic fields, Natur. Sci. Rep. Ochanomizu Univ., **29**, 1978, 37–42.
Ono,K. [99]: Indivisibility of class numbers of real quadratic fields, Compositio Math., **119**, 1999, 1–11.

Ono,T. [70]: Gauss transforms and zeta-functions, Ann. of Math., (2) **91**, 1970, 332–361.
Oozeki,K. [78]: On truncated units, TRU Math., **14**, 1978, 1–3.
Oozeki,K. [79]: On some truncated units in algebraic number fields of degree $n \geq 3$, Monatsh. Math., **87**, 1979, 310–312.
Opolka,H. [80a]: Zur Auflösung zahlentheoretischer Knoten, Math. Z., **173**, 1981, 95–103.
Opolka,H. [80b]: Auflösung zahlentheoretischer Knoten in Galoiserweiterungen von Q, Archiv Math., **34**, 1980, 416–420.
Opolka,H. [81]: Geschlechter von zentralen Erweiterungen, Archiv Math., **37**, 1981, 418–424.
Opolka,H. [82]: Some remarks on Hasse norm theorem, Proc. Amer. Math. Soc., **84**, 1982, 464–466.
Opolka,H. [84]: Normenreste in relativ abelschen Zahlkörpererweiterungen und symplektische Paarungen, Abh. Math. Sem. Univ. Hamburg, **54**, 1984, 1–4.
Opolka,H. [87]: The norm exponent in Galois extensions of number fields, Proc. Amer. Math. Soc., **99**, 1987, 41–43.
Opolka,H. [90]: Norms in finite Galois extension of the rationals, Internat. J. Math. Math. Sci., **13**, 1990, 811–812.
Opolka,H. [91]: Norm exponents and representation groups, Proc. Amer. Math. Soc., **111**, 1991, 595–597.
Oppenheim,A. [34]: Quadratic fields with and without Euclid's algorithm, Math. Ann., **109**, 1934, 349–352.
Orde,H.L.S. [78]: On Dirichlet's class number formula, J. London Math. Soc., (2) **18**, 1978, 409–420.
Ore,O. [23]: Zur Theorie der algebraischer Körper, Acta Math., **44**, 1923, 219–314.
Ore,O. [24]: Zur Theorie der Eisensteinschen Gleichungen, Math. Z., **20**, 1924, 267–279.
Ore,O. [25a]: Weitere Untersuchungen zur Theorie der algebraischen Körper, Acta Math., **45**, 1925, 145–160.
Ore,O. [25b]: Bestimmung der Diskriminanten algebraischer Körper, Acta Math., **45**, 1925, 303–344.
Ore,O. [25c]: Bestimmung der Differente eines algebraischen Zahlkörpers, Acta Math., **46**, 1925, 363–392.
Ore,O. [26a]: Bemerkungen zur Theorie der Differente, Math. Z., **25**, 1926, 1–8.
Ore,O. [26b]: Über zusammengesetzte algebraische Körper, Acta Math., **49**, 1926, 379–396.
Ore,O. [26c]: Existenzbeweise für algebraische Körper mit vorgeschriebenen Eigenschaften, Math. Z., **25**, 1926, 474–489.
Ore,O. [26d]: Über die Bedeutung der Fundamentalgleichung in der Theorie der algebraischen Körper, Math. Ann., **95**, 1926, 239–246.
Ore,O. [27]: Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, Math. Ann., **96**, 1926, 313–352; II, **97**, 1927, 569–598.
Ore,O. [28a]: Newtonsche Polygone in der Theorie der algebraischer Körper, Math. Ann., **99**, 1928, 84–117.
Ore,O. [28b]: Abriss einer arithmetischer Theorie der Galoisschen Körper, Math. Ann., **100**, 1928, 650–673; II, **102**, 1930, 283–304.
Oriat,B. [72]: Étude arithmétique des corps cycliques de degré p^r sur le corps des nombres rationnels, Enseign. Math., (2) **18**, 1972, 57–104.
Oriat,B. [76]: Relation entre le 2-groupe des classes d'idéaux au sens ordinaire et restraint de certains corps de nombres, Bull. Soc. Math. France, **104**, 1976, 301–307.

Oriat,B. [77]: Relation entre le 2-groupe des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. Inst. Fourier, **27**, 1977, no.2, 37–59.

Oriat,B. [78]: Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $Q(\sqrt{2p})$ et $Q(\sqrt{-2p})$, J. Math. Soc. Japan, **30**, 1978, 279–285.

Oriat,B. [81]: Annulation de groupe de classes réelles, Nagoya Math. J., **81**, 1981, 45–56.

Oriat,B.,Satgé,P. [79]: Un essai de généralisation du "Spiegelungssatz", J. Reine Angew. Math., **307/308**, 1979, 134–159.

Osada,H. [87]: Note on the class number of the maximal real subfield of a cyclotomic field, Manuscripta Math., **58**, 1987, 215–227; II, Nagoya Math. J., **113**, 1989, 147–151.

Ostmann,H.H. [68]: *Additive Zahlentheorie*, Springer 1968.

Ostrowski,A. [13]: Über einige Fragen der allgemeinen Körpertheorie, J. Reine Angew. Math., **143**, 1913, 255–284.

Ostrowski,A. [17]: Über sogenannte perfekte Körper, J. Reine Angew. Math., **147**, 1917, 191–204.

Ostrowski,A. [18]: Über einige Lösungen der Funktionalgleichung $\varphi(x)\varphi(y) = \varphi(xy)$, Acta Math., **41**, 1918, 271–284.

Ostrowski,A. [20]: Über Dirichletsche Reihen und algebraische Differentialgleichungen, Math. Z., **8**, 1920, 241–298.

Ostrowski,A. [35]: Untersuchungen zur arithmetischer Theorie der Körper, Math. Z., **39**, 1935, 269–320; II–III, 321–404.

Ou,Z.M.,Williams,K.S. [01]: On the density of cyclic quartic fields, Canad. Math. Bull., **44**, 2001, 97–104.

Ozaki,M.,Yamamoto,G. [01]: Iwasawa λ-invariants of certain cubic fields, Acta Arith., **97**, 2001, 387–398.

Ozaki,M.,Taya,H. [95]: A note on Greenberg's conjecture for real abelian number fields., Manuscripta Math., **88**, 1995, 311–320.

Ozaki,M.,Taya,H. [97]: On the Iwasawa λ_2-invariants of certain families of real quadratic number fields., Manuscripta Math., **94**, 1997, 437–444.

Pajunen,S. [76]: Computations on the growth of the first factor for prime cyclotomic fields, Nordisk Tidskr. Inform., **16**, 1976, 85–87; II, **17**, 1977, 113–114.

Pall,G. [45]: Note on factorization in a quadratic field, Bull. Amer. Math. Soc., **51**, 1945, 771–775.

Pall,G. [69]: Discriminantial divisors of binary quadratic forms, J. Number Theory, **1**, 1969, 525–533.

Panaitopol,L. [00]: Minorations pour les mesures de Mahler de certains pôlynomes particuliers, J. Théor. Nombres Bordeaux, **12**, 2000, 127–132.

Panella,G. [66]: Un teorema di Golod-Šafarevič e alcune sue conseguenze, Confer. Sem. Math. Univ. Bari, **104**, 1966, 1–17.

Papkov,P.S. [44]: On imaginary quadratic realms admitting only one ambiguous class, Soobshch. Akad. Nauk Gruz. SSR, **5**, 1944, 588–592. (Russian)

Pappalardi,F. [95]: On the exponent of the ideal class group of $Q(\sqrt{-d})$, Proc. Amer. Math. Soc., **123**, 1995, 663–671.

Park,Y.H. [02]: The class number one problem for the non-abelian normal CM-fields of degree 24 and 40, Acta Arith., **101**, 2002, 63–80.

Park,Y.H., Kwon,S.M. [97]: Determination of all imaginary abelian sextic number fields with class number ≤ 11, Acta Arith., **82**, 1997, 27–43.

Park,Y.H., Kwon,S.M. [98]: Determination of all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number ≤ 20, Acta Arith., **83**, 1998, 211-223.

Parry,C.J. [71a]: On a problem of Schinzel concerning principal divisors in arithmetic progressions, Acta Arith., **19**, 1971, 215–222.
Parry,C.J. [71b]: Algebraic number fields with the principal ideal condition, Acta Arith., **19**, 1971, 409–413.
Parry,C.J. [71c]: A further note on principal divisors in arithmetic progressions, J. Number Theory, **3**, 1971, 182–183.
Parry,C.J. [75a]: Units of algebraic number fields, J. Number Theory, **7**, 1975, 385–388; corr. **9**, 1977, p.278.
Parry,C.J. [75b]: Class number relations in pure quintic fields, J. Reine Angew. Math., **274/275**, 1975, 360–375.
Parry,C.J. [75c]: Pure quartic fields whose class numbers are even, J. Reine Angew. Math., **272**, 1975, 102–112.
Parry,C.J. [75d]: Class number relations in pure sextic fields, J. Reine Angew. Math., **274/275**, 1975, 360–375.
Parry,C.J. [77a]: Class number formulae for bicubic fields, Illinois J. Math., **21**, 1977, 148–163.
Parry,C.J. [77b]: Real quadratic fields with class numbers divisible by five, Math. Comp., **31**, 1977, 1019–1029.
Parry,C.J. [78]: On the class number of relative quadratic fields, Math. Comp., **32**, 1978, 1261–1270.
Parry,C.J. [80]: A genus theory for quartic fields, J. Reine Angew. Math., **314**, 1980, 40–71.
Parry,C.J. [90]: Bicyclic bicubic fields, Canad. J. Math., **42**, 1990, 491–507.
Parry,C.J.,Walter,C.D. [76]: The class number of pure fields of prime degree, Mathematika, **23**, 1976, 220–226; corr.: **24**, 1977, p.133.
Pathiaux,M. [75]: Sur le produit des conjugués à l'extérieur du cercle unité d'un nombre algébrique, Sém. Delange–Pisot–Poitou, 1975, fasc.2, exp.66.
Patterson,S.J. [87]: The distribution of general Gauss sums and similar arithmetic functions at prime arguments, Proc. London Math. Soc., (3) **54**, 1987, 193–215.
Pauli,S.,Roblot,X.-F, [01]: On the computation of all extensions of a p-adic field of a given degree, Math. Comp., **70**, 2001, 1641–1659.
Payan,J.J. [62a]: Construction des corps abéliens de degré 5, C.R. Acad. Sci. Paris, **254**, 1962, 3618–3620.
Payan,J.J. [62b]: Entiers des corps abéliens de degré 5, C.R. Acad. Sci. Paris, **255**, 1962, 2345–2347.
Payan,J.J. [65]: Contribution a l'étude des corps abéliens absolus de degré premier impair, Ann. Inst. Fourier, **15**, 1965, no.2, 133–199.
Payan,J.J. [73]: Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur Q ou sur un corps quadratique imaginaire, Ark. Mat., **11**, 1973, 239–244.
Payan,J.J. [81]: Remarques sur la structure galoisienne des unités des corps de nombres, Acta Arith., **39**, 1981, 77–82.
Pearson,K.R.,Schneider,J.E. [70]: Rings with a cyclic group of units, J. Algebra, **16**, 1970, 243–251.
Pellet,A. [78]: Sur la décomposition d'une fonction entiére en facteurs irréductibles suivant un module premier, C.R. Acad. Sci. Paris, **86**, 1878, 1071–1072.
Perlis,R. [77a]: On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory, **9**, 1977, 342–360.
Perlis,R. [77b]: A remark about zeta functions of number fields of prime degree, J. Reine Angew. Math., **293/294**, 1977, 435–436.
Perlis,R. [78]: On the class numbers of arithmetically equivalent fields, J. Number Theory, **10**, 1978, 489–509.

Perlis,R. [85]: On the analytic determination of the trace form, Canad. Math. Bull., **28**, 1985, 422–430.
Perlis,R.,Schinzel,A. [79]: Zeta functions and the equivalence of integral norms, J. Reine Angew. Math., **309**, 1979, 176–182.
Perott,J. [88]: Sur l'équation $t^2 - Du^2 = -1$, J. Reine Angew. Math., **102**, 1888, 185–223.
Perret,M. [99]: On the ideal class group problem for global fields, J. Number Theory, **97**, 1999, 27–35.
Perrin-Riou,B. [98]: Systémes d'Euler p-adiques et théorie d'Iwasawa, Ann. Inst. Fourier, **48**, 1998, 1231–1307.
Perron,O. [07]: Grundlagen fuer eine Theorie des Jacobischen Kettenbruchalgorithmus, Math. Ann., **64**, 1907, 1–76.
Perron,O. [14]: Abschätzung der Lösung der Pellschen Gleichung, J. Reine Angew. Math., **144**, 1914, 71–73.
Perron,O. [32]: Quadratische Körper mit Euklidischem Algorithmus, Math. Ann., **107**, 1932, 489–495.
Petersson,H. [55]: Über eine Zerlegung des Kreisteilungspolynoms von Primzahlordnung, Math. Nachr., **14**, 1955, 361–375.
Petersson,H. [59]: Über Darstellungsanzahlen von Primzahlen in Quadratsummen, Math. Z., **71**, 1959, 289–307.
Pethő,A. [74]: Über die Darstellung der rationalen Zahlen durch Normformen, Publ. Math. Debrecen, **21**, 1974, 31–38.
Pethő,A. [93]: Über kubische Ausnahmeeinheiten, Archiv Math., **60**, 1993, 146–153.
Pethő,A.,Pohst,M.,Williams,H.C.,Zimmer,H.G. (editors) [91]: *Computational Number Theory*, de Gruyter 1991.
Petr,K. [35]: Basis der ganzen Zahlen in algebraischen Zahlkörpern, Časopis mat.-fys., **64**, 1935, 62–72.
Pezda,T. [94a]: Polynomial cycles in certain local domains, Acta Arith., **66**, 1994, 11–22.
Pezda,T. [94b]: Cycles of polynomial mappings in several variables, Manuscripta Math., **83**, 1994, 279–289.
Pezda,T. [03]: Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals, Acta Arith., **108**, 2003, 127–146.
Phragmén,E. [92]: Sur la distribution des nombres premiers, C.R. Acad. Sci. Paris, **114**, 1892, 337–340.
Pieper,H. [72]: Die Einheitengruppe eines zahm-verzweigten galoisschen Körpers als Galois-Modul, Math. Nachr., **54**, 1972, 173–210.
Pieper,H. [73]: Die Einseinheitengruppen höheren Stufen einer zerfallenden zahmverzweigten Erweiterung als Galoismoduln, Math. Nachr., **58**, 1973, 193–200.
Pierce,S. [74]: Steinitz classes in quartic fields, Proc. Amer. Math. Soc., **43**, 1974, 39–41.
Pinner,C.G.,Vaaler,J.D. [99]: The number of irreducible factors of a polynomial, III, in: *Number Theory in Progress*, **I**, 395–405, de Gruyter 1999.
Pintz,J. [74]: On Siegel's theorem, Acta Arith., **24**, 1973/74, 543–551.
Pintz,J. [76a]: Elementary methods in the theory of L-functions, I, Hecke's theorem, Acta Arith., **31**, 1976, 53–60.
Pintz,J. [76b]: Elementary methods in the theory of L-functions, II, On the greatest zero of a real L-function, Acta Arith., **31**, 1976, 273–289.
Pintz,J. [76c]: Elementary methods in the theory of L-functions, IV, The Heilbronn phenomenon, Acta Arith., **31**, 1976, 419–429.
Pintz,J. [76d]: On the Brauer-Siegel theorem, in: *Topics in Number Theory, (Debrecen 1974*, 259–265, North-Holland 1974.

Pintz,J. [77a]: Elementary methods in the theory of L-functions, VII, Upper bound for $L(1,\chi)$, Acta Arith., **32**, 1977, 397–406; corr. **33**, 1977, 293–295.
Pintz,J. [77b]: Elementary methods in the theory of L-functions, VIII, Real zeros of real L-functions, Acta Arith., **33**, 1977, 89–98.
Pisot,C. [36]: Sur une propriété de certains entiers algébriques, C.R. Acad. Sci. Paris, **202**, 1936, 892–894.
Pisot,C. [63]: *Quelques aspects de la théorie des entiers algébriques*, Montreal 1963; 2nd ed. 1966.
Pizer,A. [76]: On the 2-part of the class-number of imaginary quadratic number fields, J. Number Theory, **8**, 1976, 184–192.
Platonov,V.P.,Drakokhrust,Ya.A. [85]: On Hasse's principle for algebraic number fields, Dokl. Akad. Nauk SSSR, **281**, 1985, 793–797. (Russian)
Pleasants,P.A.B. [74]: The number of generators of the integers of a number field, Mathematika, **21**, 1974, 160–167.
Pohst,M. [75a]: Über biquadratische Zahlkörper gleicher Diskriminante, Abh. Math. Sem. Univ. Hamburg, **43**, 1975, 192–197.
Pohst,M. [75b]: Berechnung kleiner Diskriminanten total reller algebraischer Zahlkörper, J. Reine Angew. Math., **278/279**, 1975, 278–300.
Pohst,M. [76]: Invarianten des total reellen Körpers siebten Grades mit Minimaldiskriminante, Acta Arith., **30**, 1976, 199–207.
Pohst,M. [77]: Regulatorabschätzungen für total reelle algebraische Zahlkörper, J. Number Theory, **9**, 1977, 459–492.
Pohst,M. [82]: On the computation of number fields with small discriminants including the minimum discriminants of sixth degree fields, J. Number Theory, **14**, 1982, 99–117.
Pohst,M. (editor) [87]: *Algorithmic Methods in Algebra and Number Theory*, J. Symb. Comput., **4**, 1987, no.1.
Pohst,M. [93]: *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser 1993.
Pohst,M. [94]: On computing fundamental units, J. Number Theory, **47**, 1994, 93–105.
Pohst,M. [98]: Tables of unit groups and class groups of quintic fields and a regulator bound, Math. Comp., **67**, 1998, 361–367.
Pohst,M.,Martinet,J.,Diaz y Diaz,F. [90]: The minimum discriminant of totally real octic fields, J. Number Theory, **36**, 1990, 149–159.
Pohst,M.,Weiler,P.,Zassenhaus,H. [82]: An effective computation of fundamental units, II, Math. Comp., **38**, 1982, 293–329.
Pohst,M.,Wildanger,K. [98]: Tables of unit groups and class groups of quintic fields and a regulator bound, Math. Comp., **67**, 1998, 361–367.
Pohst,M.,Zassenhaus,H. [77]: An effective number geometric method of computing the fundamental units of an algebraic number field, Math. Comp., **31**, 1977, 754–770.
Pohst,M.,Zassenhaus,H. [82]: An effective computation of fundamental units, I, Math. Comp., **38**, 1982, 275–291.
Pohst,M.,Zassenhaus,H. [89]: *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press 1989. [Reprint: Cambridge 1997.]
Poincaré,H. [92]: Extensions au nombres premiers complexes des théorèmes de M.Tchebicheff, J. math. pures appl., (4) **8**, 1892, 25–68.
Poitou,G. [76]: Sur les petits discriminants, Sém. Delange–Pisot–Poitou, **18**, 1976/7, exp.8.
Poitou,G. [77]: Minoration de discriminants (aprés Odlyzko), in: *Séminaire Bourbaki*, 136–153, Lecture Notes in Math., **567**, Springer 1977.

Pollaczek,F. [24]: Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln, Math. Z., **21**, 1924, 1–38.

Pollaczek,F. [29]: Über die Einheiten relativabelscher Zahlkörper, Math. Z., **30**, 1929, 520–551.

Pollaczek,F. [46]: Relation entre les dérivées logarithmiques de Kummer et des logarithmes π-adiques, Bull. Sci. Math., (2) **70**, 1946, 199–218.

van der Poorten,A.J.,te Riele,H.J.J.,Williams,H.C. [01]: Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less that 100 000 000 000, Math. Comp., **70**, 2001, 1311–1328; Corr.: **72**, 2003, 521–523.

van der Poorten,A.J.,Schlickewei,H.P. [91]: Additive relation in fields, J. Austral. Math. Soc., **51**, 1991, 154–170.

Popken,J. [66]: Algebraic independence of certain zêta functions, Indag. Math., **28**, 1966, 1–5.

Porusch,J. [33]: Die Arithmetik in Zahlkörpern, deren zugehörige Galoische Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Z., **37**, 1933, 134–160.

Potter,H.S.A.,Titchmarsh,E.C. [35]: The zeros of Epstein zetafunctions, Proc. London Math. Soc., (2) **35**, 1935, 372–384.

Prachar,K. [57]: *Primzahlverteilung*, Springer 1957.

Prapavessi,D.T.[91]: On Jacobi sum Hecke characters ramified only at 2, J. Number Theory, **38**, 1991, 161–184.

Prasad,D.,Yogananda,C.S. [00]: A report on Artin's conjecture, in: *Number Theory*, 301–314, Birkhäuser 2000.

Prüfer,H. [25]: Neue Begründung der algebraischen Zahlentheorie, Math. Ann., **54**, 1925, 198–243.

Puchta,J.-C. [00]: On the class number of p-th cyclotomic field, Archiv Math., **74**, 2000, 266–268.

Pumplün,D. [63]: Über Zerlegungen des Kreisteilungspolynoms, J. Reine Angew. Math., **213**, 1963, 200–220.

Pumplün,D. [65]: Über die Klassenzahl imaginär-quadratischer Zahlkörper, J. Reine Angew. Math., **218**, 1965, 23–30.

Pumplün,D. [66]: Eine Bemerkung über das Kompositum von Dedekindringen über Hauptidealringen, J. Reine Angew. Math., **222**, 1966, 214–220.

Pumplün,D. [68]: Über die Klassenzahl und die Grundeinheit des reellquadratischen Zahlkörpers, J. Reine Angew. Math., **230**, 1968, 167–210.

Purdy,G. [72]: The real zeros of the Epstein zeta function, Ph.D. thesis, Univ. of Illinois, 1972.

Quadri,M.A.,Irfan,M. [79]: A characterization of Dedekind domains, Tamkang J. Math., **10**, 1979, 165–167.

Queen,C.S. [73]: Euclidean subrings of global fields, Bull. Amer. Math. Soc., **79**, 1973, 437–439.

Queen,C.S. [76]: A note on class numbers of imaginary quadratic fields, Archiv Math., **27**, 1976, 295–298.

Quême,R. [98]: A computer algorithm for finding new Euclidean number fields, J. Théor. Nombres Bordeaux, **10**, 1998, 33–48.

Quer,J. [87]: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, C.R. Acad. Sci. Paris, **305**, 1987, 215–218.

Queyrut,J. [72]: Extensions quaternioniennes généralisées et constante de l'équation fonctionnelle des séries d'Artin, Publ. Math. Univ. Bordeaux, 1972/73, no.4, 91–119; add., *ibidem*, 1973/74, no.1, 71–72.

Queyrut,J. [81a]: Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées, I, Ann. Inst. Fourier, **31**, 1981, no.3, 1–35.

Queyrut,J. [81b]: S-groupes de Grothendieck et structure galoisienne des anneaux d'entiers, in: *Integral Representations and Applications*, 219–239, Lecture Notes in Math., **882**, Springer 1981.
Queyrut,J. [82]: S-groupes de classes d'un ordre arithmétique, J. Algebra, **76**, 1982, 234–260.
Rabinowitsch,G. [13]: Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkörpern J. Reine Angew. Math., **142**, 1913, 153–164.
Rabung,J.R. [70]: Preassigned character values in the gaussian integers, J. Number Theory, **2**, 1970, 329–332.
Rademacher,H. [35]: Primzahlen reell-quadratischer Zahlkörper in Winkelräumen, Math. Ann., **111**, 1935, 209–228.
Rademacher,H. [36a]: Über die Primzahlen eines reell-quadratischer Zahlkörpers, Acta Arith., **1**, 1936, 67–77.
Rademacher,H. [36b]: On prime numbers of real quadratic fields in rectangles, Trans. Amer. Math. Soc., **39**, 1936, 380–386.
Rados,G. [06]: Die Diskriminante der allgemeinen Kreisteilungsgleichung, J. Reine Angew. Math., **131**, 1906, 49–55.
Rados,G. [30]: Über die Verallgemeinerung eines Kroneckerschen Determinantensatzes, J. Reine Angew. Math., **162**, 1930, 198–202.
Raghavendran,R. [70]: A class of finite rings, Compositio Math., **22**, 1970, 49–57.
Ramachandra,K. [64]: Some applications of Kronecker's limit formula, Ann. of Math., (2) **80**, 1964, 104–148.
Ramachandra,K. [69]: On the class number of relative abelian fields, J. Reine Angew. Math., **236**, 1969, 1–10.
Ramachandra,K. [75]: On a theorem of Siegel, Nachr. Akad. Wiss. Göttingen, 1975, 43–47.
Ramachandra,K. [80]: One more proof of Siegel's theorem, Hardy-Ramanujan J., **3**, 1980, 25–40.
Ramakrishnan,D. [91]: On certain Artin L-series, in: *L-functions and Arithmetic (Durham 1989)*, 339–352, Cambridge University Press 1991.
Ramanathan,K.G. [59]: The zeta function and discriminant of a division algebra, Acta Arith., **5**, 1959, 277–288.
Ranum,A. [10]: The group of classes of congruent quadratic integers with respect to a composite ideal modulus. Trans. Amer. Math. Soc., **11**, 1910, 172–198.
Rausch,U. [85]: On a theorem of Dobrowolski about the product of conjugate numbers, Colloq. Math., **50**, 1985, 137–142.
Rausch,U. [90]: A summation formula in algebraic number fields and applications, I, J. Number Theory, **36**, 1990, 46–79.
Rausch,U. [94]: On the Piltz divisor problem in algebraic number fields, Acta Arith., **68**, 1994, 41–69.
Ray,G.A. [87]: Relations between Mahler's measure and values of L-series, Canad. J. Math., **39**, 1987, 694–732.
Rayner,F.J. [57]: Hensel's lemma, Quart. J. Math., Oxford ser., (2) **8**, 1957, 307–311.
Rayner,F.J. [58]: Relatively complete fields, Proc. Edinburgh Math. Soc., **11**, 1958/59, 131–133.
Razar,M.J. [77]: Central and genus class fields and Hasse norm theorem, Compositio Math., **35**, 1977, 281–298.
Rédei,L. [28]: Über die Klassenzahl des imaginären quadratischen Zahlkörpers, J. Reine Angew. Math., **159**, 1928, 210–219.
Rédei,L. [34a]: Arithmetischer Beweis des Satzes über die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math., **171**, 1934, 55–60.

Rédei,L. [34b]: Eine obere Schranke der Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörpern, J. Reine Angew. Math., **171**, 1934, 61–64.

Rédei,L. [34c]: Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math., **171**, 1934, 131–148.

Rédei,L. [35]: Über die Pellsche Gleichung $t^2 - du^2 = -1$, J. Reine Angew. Math., **173**, 1935, 193–211.

Rédei,L. [36]: Über einige Mittelwertfragen in quadratischen Zahlkörpern, J. Reine Angew. Math., **176**, 1936, 15–55.

Rédei,L. [38]: Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, J. Reine Angew. Math., **180**, 1938, 1–43.

Rédei,L. [41]: Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern, Math. Ann., **118**, 1941/43, 588–608.

Rédei,L. [44]: Über Klassengruppen und Klassenkörper algebraischer Zahlkörper, J. Reine Angew. Math., **186**, 1944/45, 80–90.

Rédei,L. [53]: Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, Acta Math. Acad. Sci. Hungar., **4**, 1953, 31–87.

Rédei,L. [60]: Über die quadratischen Zahlkörper mit Primzerlegung, Acta Sci. Math. (Szeged), **21**, 1960, 1–3.

Rédei,L.,Reichardt,H. [34]: Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math., **170**, 1934, 69–74.

Rehm,H.P.,Happle,W. [74]: Zur gruppentheoretischer Abschätzung von Idealklassenexponenten galoischer Zahlkörper, durch Exponenten geeigneter Teilkörper, J. Reine Angew. Math., **268/269**, 1974, 439–440.

Reich,A. [80]: Werteverteilung von Zetafunktionen, Archiv Math., **34**, 1980, 440–451.

Reich,A. [82]: Zur Universalität und Hypertranszendenz der Dedekindschen Zetafunktion, Abh. Braunschweig. Wiss. Ges., **33**, 1982, 197–203.

Reichardt,H. [33]: Arithmetische Theorie der kubischen Körper als Radikalkörper, Monatsh. Math. Phys., **40**, 1933, 323–350.

Reichardt,H. [34]: Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math., **170**, 1934, 75–82.

Reichardt,H. [70]: Über die 2-Klassengruppe gewisser quadratischer Zahlkörper, Math. Nachr., **46**, 1970, 71–80.

Reichardt,H.,Wegner,U. [37]: Arithmetische Charakterisierung von algebraisch auflösbaren Körpern und Gleichungen von Primzahlgrad, J. Reine Angew. Math., **178**, 1937, 1–10.

Reidemeister,K. [22]: Über die Relativklassenzahl gewisser relativquadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **1**, 1922, 27–48.

Reiner,I. [45]: On genera of binary quadratic forms, Bull. Amer. Math. Soc., **51**, 1945, 909–912.

Reiner,I. [56]: Unimodular complements, Amer. Math. Monthly, **63**, 1956, 246–247.

Reiner,I. [76]: *Class Groups and Picard Groups of Group Rings and Orders*, Providence 1976.

Reiter,C. [85]: Effective lower bounds on large fundamental units of real quadratic fields, Osaka Math. J., **22**, 1985, 755–765.

Rella,T. [20]: Über die multiplikative Darstellung von algebraischen Zahlen eines Galoisschen Zahlkörpers für den Bereich eines beliebigen Primteilers, J. Reine Angew. Math., **150**, 1920, 157–174.

Rella,T. [24a]: Bemerkungen zu Herrn Hensels Arbeit "Die Zerlegung der Primteiler eines beliebigen Zahlkörpers in einem auflösbaren Oberkörper", J. Reine Angew. Math., **153**, 1924, 108–110.

Rella,T. [24b]: Zur Newtonschen Approximationsmethode in der Theorie der p-adischen Gleichungswurzeln, J. Reine Angew. Math., **153**, 1924, 111–112.

Remak,R. [13]: Abschätzung der Lösung der Pellschen Gleichung im Anschluss an den Dirichletschen Existenzsatz, J. Reine Angew. Math., **143**, 1913, 250–254.

Remak,R. [31]: Elementare Abschätzungen von Fundamentaleinheiten und des Regulators eines algebraischen Zahlkörpers, J. Reine Angew. Math., **165**, 1931, 250–254.

Remak,R. [32]: Über die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten, J. Reine Angew. Math., **167**, 1932, 360–378.

Remak,R. [34]: Über den Euklidischen Algorithmus in reell-quadratischen Zahlkörpern, Jahresber. Deutsch. Math.-Verein., **44**, 1934, 238–250.

Remak,R. [52]: Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers, Compositio Math., **10**, 1952, 245–285.

Remak,R. [54]: Über algebraische Zahlkörper mit schwachem Einheitsdefekt, Compositio Math., **12**, 1954, 35–80.

Rémond,P. [66]: Étude asymptotique de certaines partitions dans certaines semigroupes, Ann. Sci. École Norm. Sup., (3) **83**, 1966, 343–410.

Replogle,D.R, [01]: Cyclotomic Swan subgroups and irregular indices, Rocky Mountain J. Math., **31**, 2001, 611–618.

Révesz,S.G. [83]: Irregularities in the distribution of prime ideals, I, Studia Sci. Math. Hungar., **18**, 1983, 57–67.

Reyes Sanchez,M.V. [99]: *Classical and Involutive Invariants of Krull Domains*, Kluwer 1999.

Rhin,G.,Smyth,C. [95]: On the absolute Mahler measure of polynomials having all zeros in a sector, Math. Comp., **64**, 1995, 295–304.

Rhin,G.,Smyth,C. [97]: On the Mahler measure of the composition of two polynomials, Acta Arith., **79**, 1997, 239–247.

Ribenboim,P. [79]: *13 Lectures on Fermat's Last Theorem*, Springer 1979.

Ribenboim,P. [99]: *The Theory of Classical Valuations*, Springer 1999.

Ribenboim,P. [01]: *Classical Theory of Algebraic Numbers*, Springer 2001.

Ribet,K.A. [76]: A modular construction of unramified p-extensions of $Q(\mu_p)$, Invent. math., **34**, 1976, 151–162.

Richaud,C. [66]: Sur la résolution des équations $x^2 - Ay^2 = \pm 1$, Atti Acad. Pontif. Nouvi Lincei, 1866, 177–182.

Richert,H.E. [57]: Über Dirichletreihen mit Funktionalgleichung, Publ. Inst. Math. Acad. Sci. Serbe, **11**, 1957, 73–124.

Rideout,D.E. [73]: A simplification of the formula for $L(1,\chi)$ where χ is a totally imaginary Dirichlet character of a real quadratic field, Acta Arith., **23**, 1973, 329–337.

Rieger,G.J. [57]: Über die Anzahl der Teiler der Ideale in einem algebraischen Zahlkörper, Archiv Math., **8**, 1957, 162–165.

Rieger,G.J. [58a]: Verallgemeinerung der Selbergschen Formeln auf Idealklassen mod $\mathfrak{f}$ in algebraischen Zahlkörpern, Math. Z., **69**, 1958, 183–194.

Rieger,G.J. [58b]: Ein weiterer Beweis der Selbergschen Formel für Idealklassen mod $\mathfrak{f}$ in algebraischen Zahlkörpern, Math. Ann., **134**, 1958, 403–407.

Rieger,G.J. [58c]: Über die Anzahl der Ideale in einer Idealklasse mod $\mathfrak{f}$ eines algebraischen Zahlkörpers, Math. Ann., **135**, 1958, 444–466.

Rieger,G.J. [58d]: Einige Sätze über Ideale in algebraischen Zahlkörpern, Math. Ann., **136**, 1958, 339–341.

Rieger,G.J. [58e]: Verallgemeinerung der Siebmethode von A.Selberg auf algebraische Zahlkörper, J. Reine Angew. Math., **199**, 1958, 208–214; II, **201**, 1959, 157–171; III, **208**, 1961, 79–90.
Rieger,G.J. [59]: Zur Wienerschen Methode in der Zahlentheorie, Archiv Math., **10**, 1959, 258–260.
Rieger,G.J. [60b]: Zum Sieb von Linnik, Archiv Math., **11**, 1960, 14–22.
Rieger,G.J. [61a]: On the prime ideals of smallest norm in an ideal class mod $\mathfrak{f}$ of an algebraic number field, Bull. Amer. Math. Soc., **67**, 1961, 314–315.
Rieger,G.J. [61b]: Das grosse Sieb von Linnik für algebraische Zahlen, Archiv Math., **12**, 1961, 184–187.
Rieger,G.J. [61c]: Eine Selbergsche Identität für algebraische Zahlen, Math. Ann., **145**, 1961/62, 77–80.
Rieger,G.J. [64]: Über die multiplikative Halbgruppe der Restklassen nach einem ganzen Ideal in einem algebraischen Zahlkörper und ihre Halbcharaktere, Archiv Math., **15**, 1964, 310–315,
Riemann,B. [60]: Ueber die Anzahl der Primzahlen unter einer gegebener Größe, Monatsber. Kgl. Preuß. Akad. Wiss. Berlin, 671–680.
Riese,U. [98]: Kronecker-Weber via Kummer, Exposition Math., **16**, 1998, 271–27.
Rim,D.S. [57]: Relatively complete fields, Duke Math. J., **24**, 1957, 197–200.
Ritter,J. [78]: $\mathfrak{P}$-adic fields having the same type of algebraic extensions, Math. Ann., **238**, 1978, 281–288.
Ritter,J.,Weiss,A. [97]: Cohomology of units and L-values at zero, J. Amer. Math. Soc., **10**, 1997, 513–552.
Robert,A. [74]: Des adèles; pourquoi?, Enseign. Math., (2) **20**, 1974, 133–145.
Robert,A.M. [00]: *A Course in p-adic Analysis*, Springer 2000.
Robert,G. [73]: Unités elliptiques et formules pour le nombre de classes des extensions d'un corps quadratique, Bull. Soc. Math. France, Mém. **36**, 1973, 5–77.
Robert,G. [74]: Nombres de Hurwitz et régularité des idéaux premiers, Sém. Delange–Pisot–Poitou, **16**, 1974/75, exp.21.
Robert,G. [78]: Nombres de Hurwitz et unités elliptiques, Ann. Sci. École Norm. Sup., (4) **11**, 1978, 297–389.
Robert,G. [79]: Caractéres exceptionnels, J. Number Theory, **11**, 1979, 161–170.
Roberts,D.P. [01]: Density of cubic fields discriminants, Math. Comp., **70**, 2001, 1699–1705.
Robertson,L. [98]: Power bases for cyclotomic integer rings, J. Number Theory, **69**, 1998, 98–118.
Robertson,L. [01]: Power bases for 2-power cyclotomic fields, J. Number Theory, **88**, 2001, 196–209.
Robinson,R.M. [62]: Intervals containing infinitely many sets of conjugate algebraic integers, in: *Studies in Mathematical Analysis*, 305–315, Stanford 1962.
Robinson,R.M. [64a]: Conjugate algebraic integers in real point sets. Math. Z., **84**, 1964, 415–427.
Robinson,R.M. [64b]: Algebraic equations with span less than 4, Math. Comp., **18**, 1964, 547–559.
Robinson,R.M. [64c]: Intervals containing infinitely many sets of conjugate algebraic units, Ann. of Math., (2) **80**, 1964, 411–428.
Robinson,R.M. [65]: Some conjectures about cyclotomic integers, Math. Comp., **19**, 1965, 210–217.
Robinson,R.M. [67]: On the distribution of certain algebraic integers, Math. Z., **99**, 1967, 28–41.
Robinson,R.M. [69]: Conjugate algebraic integers on a circle, Math. Z., **110**, 1969, 41–51.

Rodosskii,K.A. [56]: On the exceptional zero, Izv. Akad. Nauk SSSR, Ser. Mat., **20**, 1956, 667–672. (Russian)
Rodosskii,K.A. [80]: Euclidean rings, Dokl. Akad. Nauk SSSR, **253**, 1980, 819–822. (Russian)
Rogawski,J. [00]: The nonabelian reciprocity law for local fields, Notices Amer. Math. Soc., **47**, 2000, no.1, 35-41.
Rohrlich,D.E. [80a]: The nonvanishing of certain Hecke L-functions at the center of the critical strip, Duke Math. J., **47**, 1980, 223–232.
Rohrlich,D.E. [80b]: On the L-functions of canonical Hecke characters of imaginary quadratic fields, Duke Math. J., **47**, 1980, 547–557.
Rohrlich,D.E. [80c]: Galois conjugacy of unramified twists of Hecke characters, Duke Math. J., **47**, 1980, 695–703.
Rohrlich,D.E. [92]: Twists of Hecke L-functions, Forum Math., **4**, 1992, 625–633.
Rolletschek,H. [86]: On the number of divisions of the Euclidean algorithm applied to Gaussian integers, J. Symbolic Comp., **2**, 1986, 261–291.
Roquette,P. [57]: Einheiten und Divisorklassen in endlich erzeugten Körpern, Jahresber. Deutsch. Math.-Verein., **60**, 1957, 1–21.
Roquette,P. [67]: On class field towers, in: *Algebraic Number Theory*, 231–249, Academic Press 1967.
Roquette,P. [02]: History of valuations, Fields Institute Comm., **32**, 2002, 1–66.
Roquette,P.,Zassenhaus,H. [69]: A class rank estimate for algebraic number fields, J. London Math. Soc., **44**, 1969, 31–38.
Rosen,M. [81]: An elementary proof of the local Kronecker-Weber theorem, Trans. Amer. Math. Soc., **265**, 1981, 599–605.
Rosenbaum,K. [66]: On the multiplicative group of cyclic extensions of a local field, Vestnik LGU, **21**, 1966, no.1, 80–92. (Russian)
Rosenbaum,K. [70]: Über irreguläre zyklische Erweiterungen lokaler Körper, Math. Nachr., **43**, 1970, 143–159.
Rosenblüth,E. [34]: Die arithmetische Theorie und die Konstruktion der Quaternionenkörpern auf klassenkörpertheoretischer Grundlage, Monatsh. Math. Phys., **41**, 1934, 85–125.
Rosiński,J.,Śliwa,J. [76]: The number of factorizations in an algebraic number field, Bull. Acad. Pol. Sci., sér. sci. math. astr. phys., **24**, 1976, 821–826.
Rosser,B. [49]: Real roots of Dirichlet series, Bull. Amer. Math. Soc., **55**, 1949, 906–913; J. Res. Nat. Bur. Standards, **45**, 1950, 505–514.
Roth,R.L. [71]: On extensions of Q by square roots, Amer. Math. Monthly, **78**, 1971, 392–393.
Rubin,K. [87]: Global units and ideal class groups, Invent. math., **89**, 1987, 511–526.
Rubin,K. [91a]: Kolyvagin's system of Gauss sums, in: *Arithmetic Algebraic Geometry (Texel, 1989)*, 309-324, Progr. Math., **89**, Birkhäuser 1991.
Rubin,K. [91b]: The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. math., **103**, 1991, 25–68.
Rudin,W. [61]: Unique factorization in gaussian integers, Amer. Math. Monthly, **68**, 1961, 907–908.
Rudin,W. [62]: *Fourier Analysis on Groups*, J.Wiley 1962. [Reprint: 1990.]
Rudman,R.J. [73]: On the fundamental unit of a purely cubic field, Pacific J. Math., **46**, 1973, 253–256.
Rudman,R.J.,Steiner,R. [78]: A generalization of Berwick's unit algorithm, J. Number Theory, **10**, 1978, 16–34.
Rumely,R. [89]: *Capacity Theory on Algebraic Curves*, Lecture Notes in Math., **1378**, Springer 1989.
Rumely,R. [00]: The Fekete-Szegö theorem with splitting conditions, I, Acta Arith., **93**, 2000, 99–116; II, **103**, 2002, 347–410.

Rumely,R.,Lau,C.F.,Varley,R. [99]: Existence of the sectional capacity, Mem. Amer. Math. Soc., **145**, 2000.
Rump,S.M. [79]: Polynomial minimum root separation, Math. Comp., **33**, 1979, 327–336.
Rush,D.E. [83]: An arithmetic characterization of algebraic number fields with a given class group, Math. Proc. Cambridge Philos. Soc., **94**, 1983, 23–28.
Ruthinger,M. [07]: *Die Irreduzibilitätsbeweise der Kreisteilungsgleichung*, Dissertation, Univ. Strassburg 1907.
Ruzsa,I.Z. [99]: On Mahler's measure for polynomials in several variables, in: *Number Theory in Progress*, **I**, 431–444, de Gruyter 1999.
Rychlik,K. [24]: Zur Bewertungstheorie der algebraischer Körper, J. Reine Angew. Math., **153**, 1924, 94–107.
Rzedowski-Calderón,M.,Villa-Salvador,G. [96]: Solitary fields of low degree over Q, in: *XXVIII National Congress of the Mexican Math.Soc.*, 179–192, Mexico 1996.
Sairaiji,F.,Shimizu,K. [01]: A note on Ono's numbers associated to imaginary quadratic fields, Proc. Japan Acad. Sci., **77**, 2001, 29–31.
Sairaiji,F.,Shimizu,K. [02]: An inequality between class numbers and Ono's numbers associated to imaginary quadratic fields, Proc. Japan Acad. Sci., **78**, 2002, 105–108.
Salce,L.,Zanardo,P. [81]: Arithmetical characterization of rings of algebraic integers with cyclic ideal class group, Boll. Un. Mat. Ital., (6) **1**, 1981, 117–122.
Salem,R. [44]: A remarkable class of integers. Proof of a conjecture of Vijayaraghavan, Duke Math. J., **11**, 1944, 103–108.
Salem,R. [45]: Power series with integral coefficients, Duke Math. J., **12**, 1945, 153–172.
Salem,R. [63]: *Algebraic Numbers and Fourier Analysis*, Boston 1963.
Saltman,D.J. [84]: Retract rational fields and cyclic extensions, Israel J. Math., **47**, 1984, 165–215,
Samet,P.A. [53]: Algebraic integers with two conujugates outside the unit circle, Proc. Cambridge Philos. Soc., **49**, 1953, 421–436; II, **50**, 1954, p.346.
Samuel,P. [66]: À propos du théorème des unités, Bull. Sci. Math., (2) **90**, 1966, 94–96.
Samuel,P. [67]: *Théorie algébrique des nombres*, Paris 1967. [English translation: Boston 1970.]
Samuel,P. [71]: About euclidean rings, J. Algebra, **19**, 1971, 282–301.
Sands,J.W. [84a]: Galois groups of exponent two and the Brumer-Stark's conjecture, J. Reine Angew. Math., **349**, 1984, 129–135.
Sands,J.W. [84b]: Abelian fields and the Brumer-Stark's conjecture, Compositio Math., **53**, 1984, 337–346.
Sands,J.W. [85]: Two cases of Stark's conjecture, Math. Ann., **272**, 1985, 349–359.
Sands,J.W. [87]: Stark's conjecture and abelian L-functions with higher order zeros at $s = 0$, Adv. in Math., **66**, 1987, 62–87.
Sands,J.W. [91]: Generalization of a theorem of Siegel, Acta Arith., **58**, 1991, 47–57.
Sands,J.W.,Schwarz,W. [95]: A Demjanenko matrix for abelian fields of prime power conductor, J. Number Theory, **52**, 1995, 85–97.
Sankaranarayana,A. [95]: Zeros of quadratic zeta-functions on the critical line, Acta Arith., **69**, 1995, 21–38.
Saparniyazov,O. [65]: Asymptotic equalities for the class number of ideals in an imaginary quadratic field, Lit. Mat. Sb., **5**, 1965, 303–305. (Russian)
Sarbasov,G. [67]: Improvement of the remainder term in the asymptotical formula for the distribution of cyclic fields of prime degree l, IAN Kazakh. SSR, 1967, no.1, 61–62. (Russian)

Sarges,H. [76]: Eine Anwendung des Selbergschen Siebes auf algebraische Zahlkörper, Acta Arith., **28**, 1976, 433–455.
Sarnak,P.,Zaharescu,A. [02]: Some remarks on Landau-Siegel zeros, Duke Math. J., **111**, 2002, 495–507.
Sasaki,R. [86]: On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad. Sci., **62**, 1986, 37–39.
Sasaki,R. [88]: Generalized Ono invariant and Rabinowitsch's theorem for real quadratic fields, Nagoya Math. J., **109**, 1988, 117–124.
Sasaki,R. [90]: Criteria for the class number of real quadratic fields to be one. in: *Number Theory (Banff 1988)*, 501–508, de Gruyter 1990.
Sase,M. [98]: On a family of quadratic fields whose class numbers are divisible by five, Proc. Japan Acad. Sci., **74**, 1998, 120–123.
Satgé,P. [79a]: Corps résolubles et divisibilité de nombres de classes des idéaux, Enseign. Math., (2) **25**, 1979, 165–188.
Satgé,P. [79b]: Divisibilité du nombre de classes de certains corps cycliques, Astérisque, **61**, 1979, 193–203.
Satgé,P. [81]: Corps cubiques de discriminant donné, Acta Arith., **39**, 1981, 295–301.
Sato,K. [77]: On Artin's L-functions, J. College Eng. Nihon Univ., B, **18**, 1977, 21–22.
Sato,K. [81]: A remark concerning the prime decomposition in $Q(\zeta, \sqrt[s]{n})$, J. College Eng. Nihon Univ., B, **22**, 1981, 9–15.
Sato,K. [82]: On the divisibility of $\zeta_{K_1K_2}(s)\zeta_{K_1\cap K_2}(s)/\zeta_{K_1}(s)\zeta_{K_2}(s)$, J. College Eng. Nihon Univ., B, **23**, 1982, 41–46.
Sato,K. [83]: On a problem of R.Brauer on zeta functions, J. College Eng. Nihon Univ., B, **24**, 1983, 1–5; II, **25**, 1984, 33–39.
Sato,K. [85]: On a problem of R.Brauer on zeta functions of algebraic number fields, Proc. Japan Acad. Sci., **61**, 1985, 305–307; II, **63**, 1987, 212–214.
Sato,K. [86]: On Brauer's problem on zeta functions of algebraic number fields, J. College Eng. Nihon Univ., B, **27**, 1986, 1–4; II, ["On R.Brauer's..."], **28**, 1987, 33–36.
Saxl,J. [88]: On a question of W.Jehne concerning covering subgroups of groups and Kronecker classes of fields, J. London Math. Soc., (2) **38**, 1988, 243–249.
Schaal,W. [68]: Obere und untere Abschätzungen in algebraischen Zahlkörpern mit Hilfe des linearen Selbergschen Siebes, Acta Arith., **13**, 1968, 267–313.
Schaal,W. [70]: On the large sieve method in algebraic number fields, J. Number Theory, **3**, 1970, 249–270.
Schaal,W. [84]: Siebmethoden in algebraischen Zahlkörpern, Überblicke Math., 1984, 37–53.
Schanuel,S. [74]: An extension of Chevalley's theorem to congruences modulo prime powers, J. Number Theory, **6**, 1974, 284–290.
Schappacher,N. [88]: *Periods of Hecke Characters*, Lecture Notes in Math., **1301**, Springer 1988.
Scharaschkin,V. [99]: The Hasse principle modulo nth powers, Acta Arith., **87**, 1999, 268–285.
Scharlau,R. [80]: The fundamental unit in quadratic extensions of imaginary quadratic fields, Archiv Math., **34**, 1980, 534–537.
Scheicher,K. [97]: Kanonische Ziffernsysteme und Automaten, Grazer Math. Berichte, **333**, 1997, 1–17.
Schenkman,E. [64]: On the multiplicative group of a field, Archiv Math., **15**, 1964, 282–285.

Schertz,R. [73]: L-Reihen in imaginär-quadratischen Zahlkörpern und ihre Anwendung auf Klassenzahlprobleme bei quadratischen und biquadratischen Zahlkörpern, I, J. Reine Angew. Math., **262/263**, 1973, 120–133; II, **270**, 195–212.

Schertz,R. [74a]: Arithmetische Ausdeutung der Klassenzahlformel für einfach reelle kubische Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **41**, 1974, 211–223.

Schertz,R. [74b]: Über die Klassenzahl gewisser nicht galoischer Körper 6-ten Grades, Abh. Math. Sem. Univ. Hamburg, **42**, 1974, 217–227.

Schertz,R. [76]: Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3, J. Reine Angew. Math., **286/287**, 1976, 46–74.

Schertz,R. [77]: Die Klassenzahl der Teilkörper abelscher Erweiterungen imaginärquadratischer Zahlkörper, J. Reine Angew. Math., **295**, 1977, 151–168; **296**, 1977, 58–79.

Schertz,R. [78a]: Zur Theorie der Ringklassenkörper über imaginär-quadratischen Zahlkörpern, J. Number Theory, **10**, 1978, 70–82.

Schertz,R. [78b]: Teilkörper relativ abelscher Erweiterungen imaginärquadratischer Zahlkörper, deren Klassenzahl durch Primteiler des Körpergrades teilbar ist, J. Reine Angew. Math., **302**, 1978, 59–69.

Schertz,R. [79]: Über die analytische Klassenzahlformel für reelle abelsche Zahlkörper, J. Reine Angew. Math., **307/308**, 1979, 424–430.

Schertz,R. [81]: Über die Klassenzahl einfach reeller kubischer Zahlkörper, Acta Arith., **39**, 1981, 369–379.

Schertz,R. [89]: Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern, J. Reine Angew. Math., **398**, 1989, 105–129.

Schertz,R. [91]: Galoismodulstrukturen und elliptische Funktionen, J. Number Theory, **39**, 1991, 285–326.

Schertz,R.,Stender,H.J. [79]: Eine Abschätzung der Klassenzahl gewisser reiner Zahlkörper sechsten Grades, J. Reine Angew. Math., **311/312**, 1979, 347–355.

Schilling,O.F.G. [43]: Normal extensions of relatively complete fields, Amer. J. Math., **65**, 1943, 309–334.

Schilling,O.F.G. [50]: *The Theory of Valuations*, Amer. Math. Soc. 1950.

Schinzel,A. [66]: On a theorem of Bauer and some of its applications, **11**, 1966, 333–344; corr. **12**, 1966/67, p.425; II, **22**, 1973, 221–231.

Schinzel,A. [68]: Remarque sur le travail précedent de T.Nagell, Acta Arith., **15**, 1968/69, 245–246.

Schinzel,A. [69]: Reducibility of lacunary polynomials, I, Acta Arith., **16**, 1969, 123–159.

Schinzel,A. [73]: On the product of the conjugates outside the unit circle of an algebraic number, Acta Arith., **24**, 1973, 385–399. Addendum: **26**, 1974/75, 329–331.

Schinzel,A. [74]: On two conjectures of P.Chowla and S.Chowla concerning continued fractions, Ann. Mat. Pura Appl., (4) **98**, 1974, 111–117.

Schinzel,A. [75a]: Traces of polynomials in algebraic numbers, Norske Vid. Selsk., **6**, 1975, 1–3.

Schinzel,A. [75b]: On linear dependence of roots, Acta Arith., **28**, 1975, 161–175.

Schinzel,A. [88]: Reducibility of lacunary polynomials, VIII, Acta Arith., **50**, 1988, 91–106.

Schinzel,A.,Zassenhaus,H. [65]: A refinement of two theorems of Kronecker, Michigan J. Math., **12**, 1965, 81–85.

Schipper,R. [77]: On the behavior of ideal classes in cyclic unramified extensions of prime degree, in: *Number Theory and Algebra*, 303–309, Academic Press 1977.

Schlickewei,H.P. [90]: S-unit equations over number fields, Invent. math., **102**, 1990, 95–107.

Schlickewei,H.P. [96]: Equations in roots of unity, Acta Arith., **76**, 1996, 99–108.
Schlickewei,H.P.,Stepanov,H.P. [93]: Algorithms to construct normal bases of cyclic number fields, J. Number Theory, **44**, 1993, 30–40.
Schmal,B. [89]: Diskriminanten, Z-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern, Archiv Math., **52**, 1989, 245–257.
Schmid,L.H. [36]: Relationen zwischen verallgemeinerten Gaussschen Summen, J. Reine Angew. Math., **176**, 1936, 189–191.
Schmid,L.P.,Shanks,D. [66]: Variations on a theorem of Landau, I, Math. Comp., **20**, 1966, 551–564.
Schmid,W.A. [03a]: Half-factorial sets in elementary p-groups, Far East J. Math. Sci., to appear.
Schmid,W.A. [03b]: Arithmetic of block monoids, Math. Slovaca, to appear.
Schmidt,C.G. [79]: Grössencharaktere und relativ-Klassenzahl abelscher Zahlkörper, J. Number Theory, **11**, 1979, 128–159.
Schmidt,C.G. [80]: Über die Führer von Gaussschen Summen als Grössencharaktere, J. Number Theory, **12**, 1980, 283–310.
Schmidt,C.G. [82]: On ray class annihilators of cyclotomic fields, Invent. math., **66**, 1982, 215–230.
Schmidt,C.G. [84]: Stickelbergerideale und Kreiseinheiten zu Klassenkörpern abelscher Zahlkörper, Invent. math., **353**, 1984, 14–54.
Schmidt,F.K. [29]: Zur Theorie der algebraisch auflösbaren Polynome und Zahlkörper von Primzahlgrad, SBer. Heidelberg. Akad. Wiss., 1929, Math.-Naturw. Kl., 3–10.
Schmidt,F.K. [36]: Über die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körpern, Math. Z., **41**, 1936, 443–450.
Schmidt,W.M. [72]: Norm form equations, Ann. of Math., (2) **96**, 1972, 526–551.
Schmidt,W.M. [95]: Number fields of given degree and bounded discriminant, Astérisque, **228**, 1995, 189–195.
Schmithals,B. [80a]: Konstruktion imaginärquadratischer Körper mit unendlichen Klassenkörperturm, Archiv Math., **34**, 1980, 307–312.
Schmithals,B. [80b]: Eine Verallgemeinerung der Klassenrangabschätzung für Zahlkörper von Roquette und Zassenhaus, Archiv Math., **34**, 1980, 412–415.
Schmithals,B. [85]: Kapitulation der Idealklassen und Einheitenstruktur in Zahlkörpern, J. Reine Angew. Math., **358**, 1985, 43–60.
Schmitz,T. [16]: Abschätzung der Lösung der Pellschen Gleichung, Arch. Math. Phys., **24**, 1916, 87–88.
Schneiders,U. [97]: Estimating the 2-rank of cubic fields by Selmer groups of elliptic curves, J. Number Theory, **62**, 1997, 375–396.
Scholz,A. [29]: Zwei Bemerkungen zum Klassenkörperturm, J. Reine Angew. Math., **161**, 1929, 201–207.
Scholz,A. [30]: Über das Verhältnis von Idealklassen und Einheitengruppe in Abelschen Körpern vom Primzahlgrad, S.B. Heidelberg Akad. Wiss., Math. Nat. Kl., **3**, 1930, 31–55.
Scholz,A. [31]: Die Abgrenzungssätze für Kreiskörper und Klassenkörper, SBer. Preuß. Akad. Wiss. Berlin, **20**, 1931, 417–426.
Scholz,A. [32]: Über die Beziehungen der Klassenzahlen quadratischer Körper zueinander, J. Reine Angew. Math., **166**, 1932, 201–203.
Scholz,A. [33]: Idealklassen und Einheiten in kubischen Körpern, Monatsh. Math. Phys., **40**, 1933, 95–111.
Scholz,A. [35]: Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Z., **39**, 1935, 95–111.

Scholz,A. [36]: Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelschen Körpererweiterungen, J. Reine Angew. Math., **175**, 1936, 100–107; II, **182**, 1940, 217–234.

Scholz,A. [43]: Zur Idealtheorie in unendlichen algebraischen Zahlkörpern, J. Reine Angew. Math., **185**, 1943, 113–126.

Scholz,A.,Taussky,O. [34]: Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluss auf das Klassenkörperturmproblem, J. Reine Angew. Math., **171**, 1934, 19–41.

Schönemann,T. [46]: Von denjenigen Moduln, welche Potenzen von Primzahlen sind, J. Reine Angew. Math., **32**, 1846, 93–105.

Schoof,R. [83]: Class groups of complex quadratic fields, Math. Comp., **41**, 1983, 295–302.

Schoof,R. [86]: Infinite class field towers of quadratic fields, J. Reine Angew. Math., **372**, 1986, 209–220.

Schoof,R. [98]: Minus class groups of the fields of the lth roots of unity, Math. Comp., **67**, 1998, 1225–1245.

Schoof,R. [03]: Class numbers of real cyclotomic fields of prime conductor, Math. Comp., **72**, 2003, 913–937.

Schoof,R.,Washington,L.C. [88]: Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp., **50**, 1988, 543–556.

Schreier,O. [27]: Über eine Arbeit von Herrn Tschebotareff, Abh. Math. Sem. Univ. Hamburg, **5**, 1927, 1–6.

Schrutka v.Rechtenstamm,G. [64]: Tabelle der (relativ)-Klassenzahlen der Kreiskörper, Abh. Deutsch. Akad. Wiss., **2**, 1964, 1–64.

Schulz-Arenstorff,R. [57]: Über die zweidimensionale Verteilung der Primzahlen reell-quadratischer Körper in Restklassen, J. Reine Angew. Math., **198**, 1957, 204–220.

Schulze,V. [72]: Die Primteilerdichte von ganzzahligen Polynomen, J. Reine Angew. Math., **253**, 1972, 175–185; II, **256**, 1972, 153–162; III, **273**, 1975, 144–145.

Schulze,V. [73]: Über die Zerlegung von Primzahlen bestimmter arithmetischer Progressionen in algebraischen Zahlkörpern, J. Reine Angew. Math., **264**, 1973, 147–148.

Schulze,V. [76a]: Polynome mit nicht durch Restklassen beschreibbaren Primteilermengen, Acta Arith., **31**, 1976, 195–197.

Schulze,V. [76b]: Die Verteilung der Primteiler von Polynomen auf Restklassen, I, J. Reine Angew. Math., **280**, 1976, 122–133; II, **281**, 1976, 126–148.

Schulze,V. [81]: Kronecker-äquivalente Körpererweiterungen und p-Ränge, J. Reine Angew. Math., **328**, 1981, 9–21.

Schumann, H.G. [37]: Zum Beweis des Hauptidealsatzes, Abh. Math. Sem. Univ. Hamburg, **12**, 1937, 42–47.

Schumer,P.D. [86]: The large sieve inequality in an algebraic number field, Mathematika, **33**, 1986, 31–54.

Schur,I. [04]: Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. Reine Angew. Math., **127**, 1904, 20–50.

Schur,I. [18a]: Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, Math. Z., **1**, 1918, 377–402.

Schur,I. [18b]: Einige Bemerkungen zu der vorstehender Arbeit des Herrn Pólya: Über die Verteilung der quadratischen Reste und Nichtreste, Nachr. Ges. Wiss. Göttingen, 1918, 30–36.

Schur,I. [29a]: Zur Irreduzibilität der Kreisteilungsgleichung, Math. Z., **29**, 1929, p.463.

Schur,I. [29b]: Elementarer Beweis eines Satzes von L.Stickelberger, Math. Z., **29**, 1929, p.464.

Schur,I. [32]: Einige Bemerkungen über die Diskriminante eines algebraischen Zahlkörpers, J. Reine Angew. Math., **167**, 1932, 264–269.
Schwarz,A.,Pohst,M.,Diaz y Diaz,F. [94]: A table of quintic number fields, Math. Comp., **63**, 1994, 361–376.
Schwarz,W. [93]: Demjanenko matrix and 2-divisibility of class numbers, Archiv Math., **60**, 1993, 154–156.
Seah,E.,Washington,L.C.,Williams,H.C. [83]: The calculation of a large cubic class number with an application to real cyclotomic fields, Math. Comp., **41**, 1983, 303–305.
Segal,R. [68]: Generalized Bernoulli numbers and the theory of cyclotomic fields, Acta Math., **121**, 1968, 49–75.
Selberg,A. [92]: Old and new conjectures and results about a class of Dirichlet series, in: *Proceedings of the Amalfi Conference on Analytic Number Theory*, 367–385, Univ. Salerno 1992 = *Collected Papers*, **II**, 47–63, Springer 1991.
Selmane,S. [99]: Non-primitive number fields of degree eight and of signature $(2,3)$, $(4,2)$ and $(6,1)$ with small discriminant, Math. Comp., **68**, 1999, 333–344.
Selmane,S. [01a]: Quadratic extensions of totally real quintic fields, Math. Comp., **70**, 2001, 837–843.
Selmane,S. [01b]: Tenth degree number fields with quintic fields having one real place, Math. Comp., **70**, 2001, 845–851.
Selmer,E.S. [51]: The diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math., **85**, 1951, 203–362.
Selmer,E.S. [53]: Sufficient congruence conditions for the existence of rational points on certain cubic surfaces, Math. Scand., **1**, 1953, 113–119.
Selucký,K.,Skula,L. [81]: Irregular imaginary fields, Arch. Math. (Brno), **17**, 1981, 95–112.
Senge,H.G. [67]: Closed sets of algebraic numbers, Duke Math. J., **34**, 1967, 307–323.
Sergeev,É.A. [73]: An integral basis of algebraic fields, Mat. Zametki, **13**, 1973, 229–234. (Russian)
Serre,J.P. [58]: Modules projectifs et espaces fibrés, à fibre vectorielle, Sém. P. Dubreil, no.23, 1958.
Serre,J.P. [62]: *Corps locaux*, Paris 1962; 2nd ed. 1968. [English translation: *Local Fields*, Springer 1979.]
Serre,J.P. [66]: Existence de tour infinies de corps de classes d'aprés Golod et Safarevic, in: *Les Tendances géometriques en algébre et théorie des nombres*, 231–238, Paris 1966.
Serre,J.P. [71a]: Conducteurs d'Artin des caractéres réels, Invent. math., **14**, 1971, 173–183.
Serre,J.P. [71b]: Cohomologie des groupes discrets, Annals of Math. Studies, **70**, 1971, 77–169.
Serre,J.P. [73]: Formes modulaires et fonctions zêta p-adiques, in: *Modular Functions of One Variable*, III, 191–268, Lecture Notes in Math., **350**, Springer 1973; corr. *ibid.*, IV, 149–150, Lecture Notes in Math., **476**, Springer 1975.
Serre,J.P. [78]: Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, C.R. Acad. Sci. Paris, **286**, 1978, A1031–A1036.
Serre,J.P. [81]: Quelques applications du théorème de Chebotarev, Inst. Hautes Études Sci., Publ. Math., **54**, 1981, 323–401.
Setzer,B. [78]: Units in totally complex S_3 fields, J. Number Theory, **10**, 1978, 244–249.
Setzer,B. [80a]: The determination of all imaginary, quartic, abelian fields with class number 1, Math. Comp., **35**, 1980, 1383–1386.

Setzer,B. [80b]: Units over totally real $C_2 \times C_2$ fields, J. Number Theory, **12**, 1980, 160–175.
Shafarevich, I.R. [43]: On the introduction of a norm in topological fields, Dokl. Akad. Nauk SSSR, **40**, 1943, 133–135. (Russian)
Shafarevich, I.R. [47]: On p-extensions, Mat. Sb., **20**, 1947, 351–363. (Russian)
Shafarevich, I.R. [51]: A new proof of the Kronecker-Weber theorem, Trudy Mat. Inst. Steklov., **38**, 1951, 382–387. (Russian)
Shafarevich,I.R. [54]: Construction of fields of algebraic numbers with given solvable Galois groups, Izv. Akad. Nauk SSSR, Ser. Mat., **18**, 1954, 525–578. (Russian)
Shafarevich,I.R. [63a]: Fields of algebraic numbers, in: *Proceedings of the ICM (Stockholm 1962)*, 163–176, Djursholm 1963. (Russian)
Shafarevich,I.R. [63b]: Extensions with given ramification, Inst. Hautes Études Sci., Publ. Math., **18**, 1963, 71–95.
Shah,S.I.A. [00]: Monogenesis of the rings of integers in a cyclic sextic field of a prime conductor, Rep. Fac. Sci. Engrg. Saga Univ., **29**, 2000, 1–10.
Shah,S.I.A.,Nakahara,T. [02]: Monogenesis of the rings of integers in certain imaginary Abelian fields, Nagoya Math. J., **168**, 2002, 1–8.
Shanks,D. [69]: On Gauss's class-number problem, Math. Comp., **23**, 1969, 151–163.
Shanks,D. [72]: New types of quadratic fields having three invariants divisible by 3, J. Number Theory, **4**, 1972, 537–556.
Shanks,D. [74]: The simplest cubic fields, Math. Comp., **28**, 1974, 1137–1152.
Shannon,C.E. [56]: The zero error capacity of a noisy channel, IRF Trans. Inform. Theory, IT-2, 1956, 8-19.
Shapiro,H.N. [49]: An elementary proof of the prime ideal theorem, Comm. Pure Appl. Math., **2**, 1949, 309–323.
Shapiro,H.N.,Sparer,G.H. [91]: Minimal bases for cubic fields, Comm. Pure Appl. Math., **44**, 1991, 1121–1136.
Shell,N. [90]: *Topological Fields and Near Valuations*, M.Dekker 1990.
Shimura,G. [62]: On the class-fields obtained by complex multiplication of abelian varieties, Osaka Math. J., **14**, 1962, 33–44.
Shimura,G. [66]: A reciprocity law in non-solvable extensions, J. Reine Angew. Math., **221**, 1966, 209–220.
Shimura,G. [68]: *Automorphic Forms and Number Theory*, Lecture Notes in Math., **54**, Springer 1968.
Shimura,G. [71a]: *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten - Princeton Univ. Press 1971.
Shimura,G. [71b]: Class fields over real quadratic fields in the theory of modular functions, in: *Several Complex Variables*, 169–188, Lecture Notes in Math., **185**, Springer 1971.
Shimura,G. [72]: Class fields over real quadratic fields and Hecke operators, Ann. of Math., (2) **95**, 1972, 120–190.
Shimura,G.,Taniyama,Y. [61]: *Complex Multiplication of Abelian Varieties and its Application to Number Theory*, Tokyo 1961.
Shintani,T. [76a]: On Kronecker limit formula for real quadratic fields, Proc. Japan Acad. Sci., **52**, 1976, 355–358.
Shintani,T. [76b]: On evaluation of zeta functions of totally real algebraic number fields at non-positive integers, J. Fac. Sci. Univ. Tokyo, IA, **23**, 1976, 393–417.
Shintani,T. [77a]: On a Kronecker limit formula for real quadratic fields, J.Fac. Sci. Univ. Tokyo, IA, **24**, 1977, 167–199.
Shintani,T. [77b]: On values at $s = 1$ of certain L functions of totally real algebraic number fields, in: *Algebraic Number Theory (Kyoto)*, 201–212, Tokyo 1977.
Shintani,T. [78]: On certain ray class invariants of real quadratic fields, J. Math. Soc. Japan, **30**, 1978, 139–167.

Shintani,T. [80a]: A proof of the classical Kronecker limit formula, Tokyo J. Math., **3**, 1980, 191–199.

Shintani,T. [80b]: A remark on zeta functions of algebraic number fields, in: *Automorphic Forms, Representation Theory and Arithmetic (Bombay 1979)*, 255–260, Tata Inst. 1980.

Shintani,T. [81]: A remark on zeta functions of algebraic number fields, in: *Automorphic Forms, Representation Theory and Arithmetic*, 255–260, Tata Inst. 1981.

Shirai,S. [75]: Central class numbers in central class field towers, Proc. Japan Acad. Sci., **51**, 1975, 389–393.

Shirai,S. [78]: On the central class field mod $\mathfrak{m}$ of Galois extension of an algebraic number field, Nagoya Math. J., **71**, 1978, 61–85.

Shirai,S. [79]: On the central ideal class group of cyclotomic fields, Nagoya Math. J., **75**, 1979, 133–143.

Shiratani,K. [64]: On some relations between Bernoulli numbers and class numbers of cyclotomic fields, Mem. Fac. Sci. Kyushu Univ., A, **18**, 1964, 127–135.

Shiratani,K. [67]: Ein Satz zu den Relativklassenzahlen der Kreiskörper, Mem. Fac. Sci. Kyushu Univ., A, **21**, 1967, 132–137.

Shiratani,K. [71]: A generalization of Vandiver's congruence, Mem. Fac. Sci. Kyushu Univ., A, **25**, 1971, 144–151.

Shokrollah,M.A. [99]: Relative class number of imaginary abelian fields of prime conductor below 10 000, Math. Comp., **68**, 1999, 1717–1728.

Shparlinskii,I.E. [92]: *Computational and Algorithmic Problems in Finite Fields*, Kluwer 1992.

Shyr,J.M. [75]: On relative class numbers of certain quadratic extensions, Bull. Amer. Math. Soc., **81**, 1975, 500–502.

Shyr,J.M. [79]: Class numbers of binary quadratic forms over algebraic number fields, J. Reine Angew. Math., **307/308**, 1979, 353–364.

Siegel,C.L. [21a]: Approximation algebraischer Zahlen, Math. Z., **10**, 1921, 173–213 = *Gesammelte Abhandlungen*, **I**, 6–46, Springer 1966.

Siegel,C.L. [21b]: Darstellung total positiver Zahlen durch Quadrate, Math. Z., **11**, 1921, 246–275 = *Gesammelte Abhandlungen*, **I**, 47–76, Springer 1966.

Siegel,C.L. [22a]: Über die Diskriminanten von total reellen Körper, Nachr. Ges. Wiss. Göttingen, 1922, 17–24 = *Gesammelte Abhandlungen*, **I**, 157–164, Springer 1966.

Siegel,C.L. [22b]: Neuer Beweis für die Funktionalgleichung der Dedekindschen Zetafunktion, Math. Ann., **85**, 1922, 123–128; II, Nachr. Ges. Wiss. Göttingen, 1922, 25–31 = *Gesammelte Abhandlungen*, **I**, 113–118, 173–179. Springer 1966.

Siegel,C.L. [32]: Über Riemann's Nachlaß zur analytischen Zahlentheorie, Quellen zur Geschichte der Math., Astr., Phys., **2**, 1932, 45–80 = *Gesammelte Abhandlungen*, **I**, 275–310. Springer 1966.

Siegel,C.L. [36]: Über die Classenzahl quadratischer Zahlkörper, Acta Arith., **1**, 1936, 83–86 = *Gesammelte Abhandlungen*, **I**, 406–409, Springer 1966.

Siegel,C.L. [37]: Über die analytische Theorie der quadratischen Formen, III, Ann. of Math., **38**, 1937, 212–291 = *Gesammelte Abhandlungen*, **I**, 469–548, Springer 1966.

Siegel,C.L. [41]: Equivalence of quadratic forms, Amer. J. Math., **63**, 1941, 685–680 = *Gesammelte Abhandlungen*, **II**, 217–239, Springer 1966.

Siegel,C.L. [44]: The average measure of quadratic forms with given discriminant and signature, Ann. of Math., (2) **45**, 1944, 667–685 = *Gesammelte Abhandlungen*, II, 473–491, Springer 1966.

Siegel,C.L. [45a]: The trace of totally positive and real algebraic integers, Ann. of Math., (2) **46**, 1945, 302–312 = *Gesammelte Abhandlungen*, **III**, 1–11, Springer 1966.

Siegel,C.L. [61]: *Lectures on Advanced Analytic Number Theory*, Tata Inst., Bombay 1961; 2nd ed. 1965, 3rd ed. 1980.

Siegel,C.L. [64]: Zu zwei Bemerkungen Kummers, Nachr. Akad. Wiss. Göttingen, 1964, 51–57 = *Gesammelte Abhandlungen*, **III**, 436–442, Springer 1966.

Siegel,C.L. [68a]: Bernoullische Polynome und quadratische Zahlkörper, Nachr. Akad. Wiss. Göttingen, 1968, 7–38 = *Gesammelte Abhandlungen*, **IV**, 9–40, Springer 1979.

Siegel,C.L. [68b]: Zum Beweis des Starkschen Satzes, Invent. math., **5**, 1968, 180–191 = *Gesammelte Abhandlungen*, **IV**, 41–52, Springer 1979.

Siegel,C.L. [69a]: Abschätzung von Einheiten, Nachr. Ges. Wiss. Göttingen, 1969, 71–86 = *Gesammelte Abhandlungen*, **IV**, 66–81, Springer 1979.

Siegel,C.L. [69b]: Berechnung von Zetafunktionen an ganzzahligen Stellen, Nachr. Akad. Wiss. Göttingen, **1969**, 87–102 = *Gesammelte Abhandlungen*, **IV**, 82–97, Springer 1979. [English translation in Siegel [61], 3rd ed.]

Siegel,C.L. [70]: Über die Fouriersche Koeffizienten der Modulformen, Nachr. Akad. Wiss. Göttingen, 1970, 15–56 = *Gesammelte Abhandlungen*, **IV**, 98–139, Springer 1979.

Siegel,C.L. [72a]: Wurzeln Heckescher Zetafunktionen, Nachr. Akad. Wiss. Göttingen, 1970, 15–56 = *Gesammelte Abhandlungen*, **IV**, 214–223, Springer 1979.

Siegel,C.L. [72b]: Algebraische Abhängigkeit von Wurzeln, Acta Arith., **21**, 1972, 59–64 = *Gesammelte Abhandlungen*, **IV**, 167–172, Springer 1979.

Siegel,C.L. [73]: Normen algebraischer Zahlen, Nachr. Akad. Wiss. Göttingen, 1973, 197–215 = *Gesammelte Abhandlungen*, **IV**, 167–172, Springer 1979.

Siegel,C.L. [75]: Zur Summation von L-Reihen, Nachr. Akad. Wiss. Göttingen, 1975, 269–292 = **IV**, 305–328, Springer 1979.

Siegel,C.L. [80]: *Advanced Analytic Number Theory*, 2nd. ed., Tata Inst. 1980.

Sierpiński,W. [64]: *Elementary Theory of Numbers*, Warszawa 1964, 2nd ed. 1987.

Silverman,J.H. [84]: An inequality relating the regulator and the discriminant of a number field, J. Number Theory, **19**, 1984. 437–442.

Silverman,J.H. [94]: *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer 1994.

Silverman,J.H. [95]: Exceptional units and numbers of small Mahler measure, Experiment Math., **4**, 1995, 69–83.

Silverman,J.H. [96]: Small Salem numbers, exceptional units and Lehmer's conjecture, Rocky Mountain J. Math., **26**, 1996, 1099–1114.

Sime,P.J. [95]: On the ideal class group of real biquadratic fields, Trans. Amer. Math. Soc., **347**, 1995, 4855–4876.

Simon,D. [01]: The index of nonmonic polynomials, Indag. Math., (N.S.) **12**, 2001, 505–517.

Sinnott,W. [78]: On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math., (2) **108**, 1978, 107–134,

Sinnott,W. [80]: On the Stickelberger ideal and the circular units of an abelian field, Invent. math., **62**, 1980/81, 181–234.

Sinnott,W. [84]: On the μ-invariant of the Γ-transform of a rational function, Invent. math., **75**, 1984, 273–282.

Sinnott,W. [87]: On a theorem of L.Washington, Astérisque, **147/148**, 1987, 209–224.

Skolem,T. [23]: Integritätsbereiche in algebraischen Zahlkörpern, Skr. Oslo, 1923, nr.21, 1–37.

Skolem,T. [35]: Lösung gewisser Gleichungen in ganzen algebraischen Zahlen, insbesondere in Einheiten, Skr. Norske. Vid. Akad. Oslo, 1935, 1–19.
Skolem,T. [48]: On the existence of a multiplicative basis for an algebraic number field, Norske Vid. Selsk, Forh., **20**, 1948, 4–7.
Skolem,T. [52]: On a certain connection between the discriminant of a polynomial and the number of its irreducible factors (mod p), Norsk Mat. Tidsskr., **34**, 1952, 81–85.
Skoruppa,N.P. [93]: Quick lower bounds for regulators of number fields, Enseign. Math., (2) **39**, 1993, 137–141.
Skula,L. [70]: Divisorentheorie einer Halbgruppe, Math. Z., **114**, 1970, 113–120.
Skula,L. [72]: Eine Bemerkung zu dem ersten Fall der Fermatschen Vermutung, J. Reine Angew. Math., **253**, 1971, 1–14.
Skula,L. [75]: Über pseudoregulären Primzahlen, J. Reine Angew. Math., **277**, 1975, 37–39.
Skula,L. [76]: On c-semigroups, Acta Arith., **31**, 1976, 247–257.
Skula,L. [80]: Index of irregularity of a prime. J. Reine Angew. Math., **315**, 1980, 92–106.
Skula,L. [81]: Another proof of Iwasawa's class number formulas, Acta Arith., **39**, 1981, 1–6.
Skula,L.,Slavutskii,I.Sh. [87]: *Bernoulli Numbers. Bibliography (1713–1983)*, Brno 1987.
Slavutskii,I.Sh. [60]: On the class-number of a real quadratic field, Izv. Vyssh. Ucheb. Zaved. Mat., 1960, no.4, 173–177. (Russian)
Slavutskii,I.Sh. [61]: On the class-number of ideals of a real quadratic field with a prime discriminant, Uch. Zap. Leningr. Gos. Ped. Inst., **218**, 1961, 179–189. (Russian)
Slavutskii,I.Sh. [65a]: On Mordell's theorem, Acta Arith., **11**, 1965, 57–66.
Slavutskii,I.Sh. [65b]: Upper bound and arithmetical determination of the class number of ideals in real quadratic fields, Izv. Vyssh. Ucheb. Zaved. Mat., 1965, no.2, 161–165. (Russian)
Slavutskii,I.Sh. [66]: Generalized Voronoi's congruence and the class-number of ideals of an imaginary quadratic field, II, Izv. Vyssh. Ucheb. Zaved. Mat., 1966, no.4, 118–126. (Russian)
Slavutskii,I.Sh. [69]: The simplest proof of Vandiver's theorem, Acta Arith., **15**, 1969, 117–118.
Slavutskii,I.Sh. [72a]: Generalized Bernoulli numbers that belong to unequal characters and an extensions of Vandiver's theorem, Uch. Zap. Leningr. Gos. Ped. Inst., **496**, 1972, 61–68. (Russian)
Slavutskii,I.Sh. [72b]: Local properties of Bernoulli numbers and a generalization of the Kummer-Vandiver theorem, Izv. Vyssh. Ucheb. Zaved. Mat., 1972. no.3, 61–69. (Russian)
Slavutskii,I.Sh. [75]: Square-free numbers and the quadratic field, Colloq. Math., **32**, 1975, 291–300. (Russian)
Slavutskii,I.Sh. [86]: Mean value of L-functions and the class number of a cyclotomic field, Zap. Nauchn. Sem. LOMI, **154**, 1986, 136–143. (Russian)
Slavutskii,I.Sh. [92]: On Zimmert's estimate for the regulator of an algebraic field, Mat. Zametki, **51**, 1992, 153–155. (Russian)
Śliwa,J. [74]: Sums of distinct units, Bull. Acad. Pol. Sci., sér. sci. math. astr. phys., **22**, 1974, 11–13.
Śliwa,J. [76a]: Factorizations of distinct lengths in algebraic number fields, Acta Arith., **31**, 1976, 399–417.
Śliwa,J. [76b]: A note on factorizations in algebraic number fields, Bull. Acad. Pol. Sci., sér. sci. math. astr. phys., **24**, 1976, 313–314.

Śliwa,J. [77]: Primes which remain irreducible in a normal field, Colloq. Math., **37**, 1977, 159–165.
Śliwa,J. [82a]: On the nonessential discriminant divisor of an algebraic number field, Acta Arith., **42**, 1982, 57–72.
Śliwa,J. [82b]: Remarks on factorizations in algebraic number fields, Colloq. Math., **46**, 1982, 123–130.
Smart,N.P. [99]: Determining the small solutions to S-unit equations, Math. Comp., **68**, 1999, 1687–1699.
de Smit,B. [93]: Algebraic numbers with integral power traces, J. Number Theory, **45**, 1993, 112–116.
de Smit,B. [95]: Primitive elements in integral bases, Acta Arith., **71**, 1995, 159–170.
de Smit,B. [98]: Generating arithmetically equivalent number fields with elliptic curves, in: *Algorithmic Number Theory (Portland 1998)*, 332–339, Lecture Notes in Comput. Sci., **1423**, Springer 1998.
de Smit,B. [01]: Brauer-Kuroda relations for S-class numbers, Acta Arith., **98**, 2001, 133–146.
de Smit,B., Perlis,R. [94]: Zeta functions do not determine class numbers, Bull. Amer. Math. Soc., (N.S.) **31**, 1994, 213–215.
Smith,H.I.S. [94]: Report on the theory of numbers, *Collected Math. Papers*, **I**, 38–364, Oxford 1894.
Smith,J.H. [69]: A remark on fields with unramified composition, J. London Math. Soc., (2) **1**, 1969, 1–2.
Smith,J.H. [75]: Representability by certain norm forms over algebraic number fields, Acta Arith., **28**, 1975, 223–227.
Smyth,C.J. [70]: Closed sets of algebraic numbers in complete fields, Mathematika, **17**, 1970, 199–205.
Smyth,C.J. [71]: On the product of the conjugates outside the unit circle of an algebraic integer, Bull. London Math. Soc., (2) **3**, 1971, 169–175.
Smyth,C.J. [73]: Problem A 5931, Amer. Math. Monthly, **80**, 1973, p.949,
Smyth,C.J. [80]: On the measure of totally real algebraic integers, I, J. Austral. Math. Soc., **30**, 1080, 137–149; II, Math. Comp., **37**, 1981, 205–208.
Smyth,C.J. [81a]: A Kronecker-type theorem for complex polynomials in several variables, Canad. Math. Bull., **24**, 1981, 447–452; corr. **25**, 1982, p.504.
Smyth,C.J. [81b]: On measures of polynomials in several variables, Bull. Austral. Math. Soc., **23**, 1981, 49–63.
Smyth,C.J. [82]: Conjugate algebraic numbers on conics, Acta Arith., **40**, 1982, 333–346.
Smyth,C.J. [84a]: Totally positive algebraic integers of small trace, Ann. Inst. Fourier, **34**, 1984, no.3, 1–28.
Smyth,C.J. [84b]: The mean values of totally real algebraic integers, Math. Comp., **42**, 1984, 663–681.
Snaith,V. [82]: A topological "proof" of a theorem of Ribet, in: *Current Trends in Algebraic Topology*, I, 43–47, Amer. Math. Soc. 1982.
Snaith,V. [94]: *Galois Module Structure*, Amer. Math. Soc. 1994.
Snaith,V. [95a]: Cyclotomic Galois module structure and the second Chinburg invariant, Math. Proc. Cambridge Philos. Soc., **117**, 1995, 57–92.
Snaith,V. [95b]: The second Chinburg invariant for cyclotomic fields via the Hom-description, C.R. Math. Rep. Acad. Sci. Canada **17**, 1995, 25–30.
Sodaïgui,B. [88]: Structure galoisienne des anneaux d'entiers, J. Number Theory, **28**, 1988, 189–204.
Sodaïgui,B. [97]: Classes réalisables par des extensions métacycliques nonabéliennes et éléments de Stickelberger, J. Number Theory, **65**, 1997, 87–95.

Sodaïgui,B. [99]: Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement, Illinois J. Math., **43**, 1999, 47–60.
Sodaïgui,B. [00a]: Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8, J. Algebra, **223**, 2000, 367–378.
Sodaïgui,B. [00b]: Realizable classes of quaternion extensions of degree $4l$, J. Number Theory, **80**, 2000, 304–315.
Sokolovskiĭ,A.V. [66]: Density theorems for a class of zeta functions, IAN Uzbek. SSR, **10**, 1966, no.3, 33–40.(Russian)
Sokolovskiĭ,A.V. [68]: A theorem on the zeros of Dedekind's zeta function and the distance between "neighbouring" prime ideals, Acta Arith., **13**, 1967/68, 321–334. (Russian)
Sokolovskiĭ,A.V. [71]: On small differences between "neighbouring" prime ideals, Dokl. Akad. Nauk SSSR, **196**, 1971, 53–56. (Russian)
Solderitsch,J.J. [92]: Quadratic fields with special class groups, Math. Comp., **59**, 1992, 633–638.
Sommer,J. [07]: *Vorlesungen über Zahlentheorie*, Teubner, 1907.
Somodi,M. [02]: Linear forms and arithmetic equivalence, Acta Arith., **105**, 2002, 1–7.
Sonn,J. [83]: Direct summands of class groups, J. Number Theory, **17**, 1983, 343–349.
Sonn,J. [85]: On equivalence of number fields, Israel J. Math., **52**, 1985, 239–244; corr. **71**, 1990, p.379.
Soulé,C. [99]: Perfect forms and the Vandiver conjecture, J. Reine Angew. Math., **517**, 1999, 209–221.
Soundararajan,K. [00]: Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc., (2) **61**, 2000, 681–690.
Soundararajan,K. [03]: Degree 1 elements of the Selberg class, preprint 2003.
Soverchia,E. [02]: Relative integral basis over a Hilbert class field, J. Number Theory, **97**, 2002, 199–203.
Späth,H. [27]: Über die Irreduzibilität der Kreisteilungsgleichung, Math. Z., **26**, 1927, 442–444.
Spearman,B.K.,Williams,K.S. [88]: Cyclic quartic fields with relative integral bases over their quadratic subfields, Proc. Amer. Math. Soc., **103**, 1988, 687–694.
Spearman,B.K.,Williams,K.S. [96a]: Normal relative integral bases for quartic fields over quadratic subfields, Kodai Math. J., **19**, 1996, 293–307.
Spearman,B.K.,Williams,K.S. [96b]: Relative integral bases for quartic fields over quadratic subfields, Acta Math. Acad. Sci. Hungar., **70**, 1996, 185–192,
Spearman,B.K.,Williams,K.S. [96c]: The conductor of a cyclic quartic field, Publ. Math. Debrecen, **48**, 1996, 13–43.
Spearman,B.K.,Williams,K.S. [98]: An explicit integral basis for a pure cubic field, Far East J.Math.Sci., **6**, 1998, 1–14.
Spearman,B.K.,Williams,K.S. [01a]: Integers which are discriminants of bicyclic or cyclic quartic fields, JP J. Algebra, Number Theory and Appl., **1**, 2001, 179–194.
Spearman,B.K.,Williams,K.S. [01b]: Cubic fields with a power basis, Rocky Mountain J. Math., **31**, 2001, 1103–1109.
Spearman,B.K.,Williams,K.S. [02a]: The discriminant of dihedral quintic field defined by a trinomial $X^5 + aX + b$, Canad. Math. Bull., **45**, 2002, 138–153.
Spearman,B.K.,Williams,K.S. [02b]: Cubic fields with index 2, Monatsh. Math., **134**, 2002, 331–336.
Speiser,A. [16]: Gruppendeterminante und Körperdiskriminante, Math. Ann., **77**, 1916, 546–562.
Speiser,A. [19]: Die Zerlegungsgruppe, J. Reine Angew. Math., **149**, 1919, 174–188.

Spencer,J. [77]: An elementary proof of Kronecker's theorem, Fibonacci Quart., **15**, 1977, 9–10.
Sprindzhuk,V.G. [73]: Square-free divisors of polynomials and the number of classes of ideals in algebraic number fields, Acta Arith., **24**, 1973, 143–149. (Russian)
Sprindzhuk,V.G. [74a]: The distribution of the fundamental units of real quadratic fields, Acta Arith., **25**, 1974, 405–409.
Sprindzhuk,V.G. [74b]: "Almost every" algebraic number field has a large class-number, Acta Arith., **25**, 1974, 405–409.
Sprindzhuk,V.G. [82]: *Classical Diophantine Equations in Two Unknowns*, Nauka, Moskva 1982. (Russian) [English translation: Springer 1993].
Springer,T.A. [57]: Note on quadratic forms over algebraic number fields, Indag. Math., **19**, 1957, 39–43.
Srinivasan,A. [98]: Computations of class numbers of real quadratic fields, Math. Comp., **67**, 1998, 1285–1308.
Srinivasan,A. [99]: Prime producing polynomials: proof of a conjecture by Mollin and Williams, Acta Arith., **89**, 1999, 1-7.
Srivastav,A.,Venkataraman,S. [97]: Unramified quadratic extensions of real quadratic fields, normal integral bases, and 2-adic L-functions, J. Number Theory, **67**, 1996, 139–145.
Stankus,E. [76]: Distribution of Dirichlet L-functions with real characters in the half-plane Re $s > 1/2$, Lit. Mat. Sb., **15**, 1975, no.4, 199–214. (Russian)
Stark,H.M. [66]: On complex quadratic fields with class number equal to one, Trans. Amer. Math. Soc., **122**, 1966, 112–119.
Stark,H.M. [67a]: There is no tenth complex quadratic field with class number one, Proc. Nat. Acad. Sci. U.S.A., **57**, 1967, 216–221.
Stark,H.M. [67b]: A complete determination of the complex quadratic fields of class-number one, Michigan J. Math., **14**, 1967, 1–27.
Stark,H.M. [69a]: On the "gap" in a theorem of Heegner, J. Number Theory, **1**, 1969, 16–27.
Stark,H.M. [69b]: A historical note on complex quadratic fields with class-number one, Proc. Amer. Math. Soc., **21**, 1969, 254–255.
Stark,H.M. [69c]: The role of modular functions in a class-number problem, J. Number Theory, **1**, 1969, 252–260.
Stark,H.M. [71]: A transcendence theorem for class-number problems, Ann. of Math., (2) **94**, 1971, 174–209.
Stark,H.M. [74]: Some effective cases of the Brauer-Siegel theorem, Invent. math., **23**, 1974, 135–152.
Stark,H.M. [75a]: L-functions at $s = 1$; II, Artin L-functions with rational characters, Adv. in Math., **17**, 1975, 60–92.
Stark,H.M. [75b]: On complex quadratic fields with class-number two, Math. Comp., **29**, 1975, 289–302.
Stark,H.M. [75c]: The analytic theory of algebraic numbers, Bull. Amer. Math. Soc., **81**, 1975, 961–972.
Stark,H.M. [76a]: L-functions at $s = 1$; III, Totally real fields and Hilbert's twelfth problem, Adv. in Math., **22**, 1976, 64–84.
Stark,H.M. [76b]: The genus theory of number fields, Comm. Pure Appl. Math., **29**, 1976, 805–811.
Stark,H.M. [77a]: Class fields for real quadratic fields and L-series at $s = 1$, in: *Algebraic Number Fields*, 355–375. London 1977.
Stark,H.M. [77b]: Class fields and modular forms of weight one, in: *Modular Functions of One Variable*, V, 277–287, Lecture Notes in Math., **601**, Springer 1977.
Stark,H.M. [80]: L-functions at $s = 1$; V, First derivative at $s = 0$, Adv. in Math., **35**, 1980, 197–235.

Stark,H.M. [82]: Values of zeta and L-functions, Abh. Braunschw. Wiss. Ges., **33**, 1982, 71–83.

Staś,W. [59]: Über eine Anwendung der Methode von Turán auf die Theorie des Restgliedes in Primidealsatz, Acta Arith., **5**, 1959, 179–195.

Staś,W. [60]: Über einige Abschätzungen in Idealklassen, Acta Arith., **6**, 1960, 1–10.

Staś,W. [61]: On a certain evaluation of the remainder in the theorem on the distribution of prime ideals, Prace Mat., **5**, 1961, 53–60. (Polish)

Staś,W. [76]: On the order of Dedekind zeta-functions in the critical strip, Funct. Approx. Comment. Math., **4**, 1976, 19–26.

Staś,W. [79]: On the order of Dedekind zeta-functions near the line $\sigma = 1$, Acta Arith., **35**, 1979, 195–202.

Staś,W.,Wiertelak,K. [75]: On some estimates in the theory of $\zeta(s,\chi)$ functions, Acta Arith., **26**, 1974/75, 293–301.

Staś,W.,Wiertelak,K. [76a]: An equivalence in ideal classes of algebraic number fields, Funct. Approx. Comment. Math., **2**, 1976, 219–232.

Staś,W.,Wiertelak,K. [76b]: Further applications of Turán's methods to the distribution of prime ideals in ideal classes mod $\mathfrak{f}$, Acta Arith., **31**, 1976, 153–165.

Stauffer,R. [36]: The construction of a normal basis in a separable extension field, Amer. J. Math., **58**, 1936, 585–597.

Steckel,H.D. [82a]: Abelsche Erweiterungen mit vorgegebenen Zahlknoten, J. Reine Angew. Math., **330**, 1982, 93–99.

Steckel,H.D. [82b]: Arithmetik in Frobeniuserweiterungen, Manuscripta Math., **39**, 1982, 359–386.

Steckel,H.D. [83]: Dichte von Frobeniuskörpern bei fixiertem Kernkörper, J. Reine Angew. Math., **343**, 1983, 39–63.

Steffan,J. [86]: Longeurs de décomposition en produits d'éléments irréductibles dans un anneau de Dedekind, J. Algebra, **102**, 1986, 229–236.

Stein,A. [27]: Die Gewinnung der Einheiten in gewissen relativquadratischen Zahlkörpern durch das J.Hurwitzsche Kettenbruchverfahren, J. Reine Angew. Math., **156**, 1927, 69–92.

Stein,S.K. [77]: Modified linear dependence and the capacity of a cyclic graph, Linear Algebra Appl., **17**, 1977, 191–195.

Steinbacher,F. [11]: Abelsche Körper als Kreisteilungskörper, J. Reine Angew. Math., **139**, 1911, 85–100.

Steiner,R.,Rudman,R. [76]: On an algorithm of Billevich for finding units in algebraic fields, Math. Comp., **30**, 1976, 598–609.

Steinig,J. [66]: On Euler's idoneal numbers, Elem. Math., **21**, 1966, 73–88.

Steinitz,E. [10]: Algebraische Theorie der Körper, J. Reine Angew. Math., **137**, 1910, 167–309. [Reprint: de Gruyter 1930.]

Steinitz,E. [12]: Rechteckige Systeme und Moduln in algebraischen Zahlkörpern, Math. Ann., **71**, 1912, 328–354; II, **72**, 1912, 297–345.

Stender,H.J. [69]: Über die Grundeinheit für spezielle unendliche Klassen rein kubischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **33**, 1969, 203–215.

Stender,H.J. [72]: Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper, J. Reine Angew. Math., **257**, 1972, 151–178.

Stender,H.J. [73]: Grundeinheiten für einige unendlichen Klassen reiner biquadratischer Zahlkörper mit einer Anwendung auf die diophantische Gleichung $x^4 - ay^4 = \pm c$ ($c = 1, 2, 4$ oder 8), J. Reine Angew. Math., **264**, 1973, 207–220.

Stender,H.J. [74]: Über die Einheitengruppe der reinen algebraischen Zahlkörper sechsten Grades, J. Reine Angew. Math., **268/269**, 1974, 78–93.

Stender,H.J. [75]: Eine Formel für Grundeinheiten in reinen algebraischen Zahlkörpern dritten, vierten und sechsten Grades, J. Number Theory, **7**, 1975, 235–250.

Stender,H.J. [77]: Lösbare Gleichungen $ax^n - by^n = c$ und Grundeinheiten für einige algebraische Zahlkörper vom Grade $n = 3, 4, 6$, J. Reine Angew. Math., **290**, 1977, 24–62.

Stender,H.J. [78]: "Verstümmelte" Grundeinheiten für biquadratische und bikubische Zahlkörper, Math. Ann., **232**, 1978, 55–64.

Stender,H.J. [83]: Einheitenbasen für parametrisierte Zahlkörper vierten und achten Grades mit beliebigen reell-quadratischen Teilkörpern, J. Number Theory, **17**, 1983, 246–269.

Stephens,A.J.,Williams,H.C. [88]: Computation of real quadratic fields with class number one, Math. Comp., **51**, 1988, 809–824,

Stephens,P.J. [72]: Optimizing the size of $L(1, \chi)$, Proc. London Math. Soc., (3) **24**, 1972, 1–14.

Stern,L. [89]: On the norm groups of global fields, J. Number Theory, **32**, 1989, 203–219.

Stern,L. [90]: On the equality of norm groups of global fields, J. Number Theory, **36**, 1990, 108–126,

Stern,L. [99]: On an obstruction to the Hasse norm principle and the equality of norm groups of algebraic number fields, J. Number Theory, **75**, 1999, 237–261.

Stevenhagen,P. [89]: Ray class groups and governing fields, Publ.Math. Fac. Sci. Besançon, 1988/89.

Stevenhagen,P. [94a]: Class number parity for the pth cyclotomic field, Math. Comp., **63**, 1994, 773–784.

Stevenhagen,P. [94b]: Extensions of homomorphisms and the structure of ray class groups, J. Algebra, **163**, 1994, 832–860.

Stevenhagen,P. [95]: A density conjecture for the negative Pell equation, in: *Computational Algebra and Number Theory (Sydney 1992)*, 187–200, Kluwer 1995.

Stewart,C.L. [78]: Algebraic integers whose conjugates lie near the unit circle, Bull. Soc. Math. France, **106**, 1978, 169–176.

Stewart,I.,Tall,D. [79]: *Algebraic Number Theory*, London– New York 1979, 2nd ed. 1987; 3rd ed.: *Algebraic Number Theory and Fermat's Last Theorem*, Peters 2002.

Stickelberger,L. [90]: Über eine Verallgemeinerung der Kreisteilung, Math. Ann., **37**, 1890, 321–367.

Stickelberger,L. [97]: Ueber eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, I Math. Kongress, Zürich 1897, 182–193.

Stiemke,E. [26]: Über unendliche algebraische Zahlkörper, Math. Z., **25**, 1926, 9–39.

Stuart,D.,Perlis,R. [95]: A new characterization of arithmetic equivalence, J. Number Theory, **53**, 1995, 300–308.

Suetuna,Z. [25a]: Über die Maximalordnung einiger Funktionen in der Idealtheorie, Japan J. Math., **1**, 1924, 69–82.

Suetuna,Z. [25b]: On the product of L-functions, Japan J. Math., **2**, 1925, 19–32.

Suetuna,Z. [28]: Über die Idealnormen eines algebraischen Körpers, J. Fac. Sci. Univ. Tokyo, **1**, 1928, 417–434; Bemerkung: 435–437.

Suetuna,Z. [29]: Über die Anzahl der Idealfaktoren von n in einem algebraischen Zahlkörper, J. Fac. Sci. Univ. Tokyo, **2**, 1929, 1–24.

Suetuna,Z. [31]: Über die Anzahl der Idealteilern, J. Fac. Sci. Univ. Tokyo, **2**, 1931, 155–177.

Suetuna,Z. [35]: Über die L-Funktionen in einem kubischen Körper, Proc. Japan Acad. Sci., **11**, 1935, 132–134.

Suetuna,Z. [36]: Über die L-Funktionen in gewissen algebraischen Zahlkörpern, Japan J. Math., **13**, 1936, 27–28.

Suetuna,Z. [37]: Abhängigkeit der L-Funktionen in gewissen algebraischen Zahlkörpern, J. Reine Angew. Math., **177**, 1937, 6–12; II, J. Fac. Sci. Univ. Tokyo, **3**, 1937, 223–252.

Sueyoshi,Y. [84]: Ramification numbers of cyclic p-extensions over $\mathfrak{p}$-adic number fields, Mem. Fac. Sci. Kyushu Univ., **38**, 1984, 163–168.

Sueyoshi,Y. [97]: On a comparison between 4-ranks of the narrow ideal class groups of $Q(\sqrt{m})$ and $Q(\sqrt{-m})$, Mem. Fac. Sci. Kyushu Univ., **51**, 1997, 261–272.

Sunley,J.S. [79]: Prime discriminants in real quadratic fields of narrow class number one, in: *Number Theory, Carbondale 1979*, 294–301, Lecture Notes in Math., **751**, Springer 1979.

Suzuki,H. [91]: A generalization of Hilbert's theorem 94, Nagoya Math. J., **121**, 1991, 161–169.

Swan,R.G. [60]: Induced representations and projective modules, Ann. of Math., (2) **71**, 1960, 552–578.

Swan,R.G. [62]: Factorizations of polynomials over finite fields, Pacific J. Math., **12**, 1962, 1099–1106.

Swift,J.D. [48]: Note on discriminants of binary quadratic forms with a single class in each genus, Bull. Amer. Math. Soc., **54**, 1948, 560–561.

Swinnerton-Dyer,H.P.F. [62]: Two special cubic surfaces, Mathematika, **9**, 1962, 54–56.

Swinnerton-Dyer,H.P.F. [01]: *A Brief Guide to Algebraic Number Theory*, Cambridge 2001.

Szegö,G. [15]: Ein Grenzwertsatz über die Toeplitzsche Determinanten einer reellen positiven Funktion, Math. Ann., **76**, 1915, 490–503.

Szegö,G.,Walfisz,A. [27]: Über das Piltzsche Teilerproblem in algebraischen Zahlkörpern, Math. Z., **26**, 1927, 138–156; II, 467–486.

Szekeres,G. [74]: On the number of divisors of $x^2 + x + A$, J. Number Theory, **6**, 1974, 434–442.

Szydło,B. [89]: Über Vorzeichenwechsel einiger arithmetischr Funktionen, Monatsh. Math., **108**, 1989, 325–336. æ

Takagi,T. [20]: Über eine Theorie des relativ-Abelschen Zahlkörpers, J. Coll. Sci. Tokyo, **41**, 1920, nr.9, 1–133.

Takagi,T. [27]: Zur Theorie des Kreiskörpers, J. Reine Angew. Math., **157**, 1927, 230–238.

Takahashi,S. [64]: An explicit representation of the generalized principal ideal theorem for the rational ground field, Tôhoku Math. J., (2) **16**, 1964, 176–182.

Takahashi,S. [65]: On Tannaka-Terada's principal ideal theorem for rational ground field, Tôhoku Math. J., (2) **17**, 1965, 87–104.

Takaku,A. [71]: Units of real quadratic fields, Nagoya Math. J., **44**, 1971, 51–55.

Takaku,A. [75]: Elementary proof of "The class number of $Q(\sqrt{l})$ is odd when l is a prime", Bull. Sci. Univ. Ryukyus, **19**, 1975, 51–55.

Takenouchi,T. [13]: On the classes of congruent integers in an algebraic körper, J. Coll. Sci. Tokyo, **36**, 1913, 1–13.

Taketa,K. [32]: Neuer Beweis eines Satzes von Herrn Furtwängler über die metabelschen Gruppen, Japan J. Math., **9**, 1932, 199–218.

Takeuchi,K. [99]: Totally real algebraic number fields of degree 9 with small discriminant, Saitama Math. J., **17**, 1999, 63–85.

Takeuchi,T. [79]: Note on the class field towers of cyclic fields of degree l, Tôhoku Math. J., (2) **31**, 1979, 301–307.

Takeuchi,T. [80]: On the l-class field towers of cyclic fields of degree l, Sci. Rep. Niigata Univ., A, **17**, 1980, 23–25.

Takhtayan,L.A.,Vinogradov,A.I. [82]: The Gauss-Hasse hypothesis on real quadratic fields with class number one, J. Reine Angew. Math., **335**, 1982, 40–86.

Tamagawa,T. [51]: On the theory of ramification groups and conductors, Japan J. Math., **21**, 1951, 197–215.
Tamagawa,T. [53]: On the functional equation of the generalized L-function, J.Fac. Sci. Univ. Tokyo, **6**, 1953, 421–428.
Tang,J.E. [91]: Quartic normal extensions of the rational field, J. Austral. Math. Soc., **51**, 1991, 473–482.
Tang,S.-L, [96]: Iwasawa invariants of real abelian number fields, J. Number Theory, **56**, 1996, 336–342.
Taniyama,Y. [57]: L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, **9**, 1957, 330–366.
Tannaka,T. [33a]: Über einen Satz von Herrn Artin, Proc. Imp. Acad. Tokyo, **9**, 1933, 197–198.
Tannaka,T. [33b]: Ein Hauptidealsatz relativ-Galoisscher Zahlkörper und ein Satz über den Normenrest, Proc. Imp. Acad. Tokyo, **9**, 1933, 355–356; Japan J. Math., **10**, 1934, 183–189.
Tannaka,T. [34]: Einige Bemerkungen zu den Arbeiten über den allgemeinen Hauptidealsatz, Japan J. Math., **10**, 1934, 163–167.
Tannaka,T. [49]: An alternative proof of a generalized principal ideal theorem, Proc. Japan Acad. Sci., **25**, 1949, 26–31.
Tannaka,T. [50]: Some remarks concerning principal ideal theorem, Tôhoku Math. J., (2) **1**, 1950, 270–278.
Tannaka,T. [56]: On the generalized principal ideal theorem, in: *Proceedings of the International Symposium on Algebraic Number Theory*, 65–77, Tokyo 1956.
Tannaka,T. [58]: A generalized principal ideal theorem and a proof of a conjecture of Deuring, Ann. of Math., (2) **67**, 1958, 574–589.
Tannaka,T.,Terada,F. [49]: A generalization of the principal ideal theorem, Proc. Japan Acad. Sci., **25**, 1949, 7–8.
Tanner,J.W., Wagstaff,S.S. [87]: New congruences for the Bernoulli numbers, Math. Comp., **48**, 1987, 341–350.
Tano,F. [89]: Sur quelques théorèmes de Dirichlet, J. Reine Angew. Math., **105**, 1889, 160–169.
Tasaka,T. [70]: Remarks on the validity of Hasse's norm theorem, J. Math. Soc. Japan, **22**, 1970, 330–341.
Tate,J. [50]: *Fourier Analysis in Number Fields and Hecke's Zeta Function*, Ph.D. thesis, Princeton Univ. 1950. [Reproduced in Cassels, Fröhlich [67]].
Tate,J. [77]: Local constants, in: *Algebraic Number Fields*, 89–131, London 1977.
Tate,J. [81a]: On Stark's conjectures on the behavior of $L(s,\chi)$ at $s = 0$, J. Fac. Sci. Univ. Tokyo, I A **28**, 1981, 963–978.
Tate,J. [81b]: Brumer-Stark-Stickelberger, Sém. Théor. Nombres Bordeaux, 1980-1981, exp.24.
Tate,J. [84]: *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, Progr. Math., **47**, Birkhäuser 1984.
Tateyama,K. [82a]: On the ideal class groups of some cyclotomic fields, Proc. Japan Acad. Sci., **58**, 1982, 333–335.
Tateyama,K. [82b]: Maillet's determinant, Sci. Papers College Gen. Edu. Univ. Tokyo, **32**, 1982, 97–100.
Tatuzawa,T. [51]: On a theorem of Siegel, Japan J. Math., **21**, 1951, 163–178.
Tatuzawa,T. [53]: On the product of $L(1,\chi)$, Nagoya Math. J., **5**, 1953, 105–111.
Tatuzawa,T. [73a]: On the number of integral ideals in algebraic number fields, whose norms not exceed x, Sci, Papers College Gen. Ed. Univ. Tokyo, **23**, 1973, 73–86.
Tatuzawa,T. [73b]: On the extended Hecke theta-formula, Trudy Mat. Inst. Steklov., **132**, 1973, 206–210.

Tatuzawa,T. [73c]: On the conductor-discriminant formula, J. Reine Angew. Math., **262/263**, 1973, 436–440.
Tatuzawa,T. [77]: On the number of integral ideals whose norms belong to some norm residue class mod q, Sci. Papers College Gen. Ed. Univ. Tokyo, **27**, 1977, 1–8.
Taussky,O. [32]: Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper, J. Reine Angew. Math., **168**, 1932, 193–210.
Taussky,O. [37a]: A remark on the class field tower, J. London Math. Soc., **12**, 1937, 82–85.
Taussky,O. [37b]: A remark on unramified class fields, J. London Math. Soc., **12**, 1937, 86–88.
Taussky,O. [49]: On a theorem of Latimer and MacDuffee, Canad. J. Math., **1**, 1949, 300–302.
Taussky,O. [51]: Classes of matrices and quadratic fields, Pacific J. Math., **1**, 1951, 127–132; II, J. London Math. Soc., **27**, 1952, 237–239.
Taussky,O. [57]: On matrix classes corresponding to an ideal and its inverse, Illinois J. Math., **1**, 1957, 108–113.
Taussky,O. [60]: Matrices of rational integers, Bull. Amer. Math. Soc., **66**, 1960, 327–345.
Taussky,O. [62]: Ideal matrices, Archiv Math., **13**, 1962, 275–282; II, Math. Ann., **160**, 1963, 218–225.
Taussky,O. [69]: A remark concerning Hilbert's theorem 94, J. Reine Angew. Math., **239/240**, 1969, 435–438.
Taussky,O. [71]: Hilbert's theorem 94, in: *Computers in Number Theory*, 65–71, Academic Press 1971.
Taussky,O. [77a]: Norms from quadratic fields and their relation to non-commuting 2×2 matrices, II, The principal genus, Houston J. Math., **3**, 1977, 543–547;
Taussky,O. [77b]: Norms from quadratic fields and their relation to non-commuting 2×2 matrices, III, A link between the 4-rank of the ideal class groups in $Q(\sqrt{m})$ and $Q(\sqrt{-m})$, Math. Z., **154**, 1977, 91–95.
Taussky,O. [80]: Some facts concerning integral representations of ideals in an algebraic number field, Linear Algebra Appl., **31**, 1980, 245–248.
Taussky,O.,Todd,J. [40]: A characterization of algebraic numbers, Proc. Roy. Irish Acad., A., **46**, 1940, 1–8.
Taya,H. [99]: On p-adic L-functions and Z_p-extensions of certain real abelian number fields, J. Number Theory, **75**, 1999, 170–184.
Taylor,M.J. [75]: Galois module structure of classgroups and units, Mathematika, **22**, 1975, 156–160.
Taylor,M.J. [78a]: On the self-duality of a ring of integers as a Galois module, Invent. math., **46**, 1978, 173–177.
Taylor,M.J. [78b]: Galois module structure of integers of relative abelian extensions, J. Reine Angew. Math., **303/304**, 1978, 97–101.
Taylor,M.J. [80a]: Galois module structure of rings of integers, Ann. Inst. Fourier, **30**, no.3, 1980, 11–48.
Taylor,M.J. [80b]: Galois module structure of rings of integers in Kummer extensions, Bull. London Math. Soc., **12**, 1980, 96–98.
Taylor,M.J. [81a]: On Fröhlichs conjecture for rings of integers of tame extensions, Invent. math., **63**, 1981, 41–79.
Taylor,M.J. [81b]: Monomial representations and rings of integers, J. Reine Angew. Math., **324**, 1981, 127–135.
Taylor,M.J. [81c]: Galois module type congruences for values of L-functions, J. London Math. Soc., (2) **24**, 1981, 441–448.

Taylor,M.J. [82a]: Galois module structure of rings of integers, in: *Journées Arithmétiques 1980*, 218–225. Cambridge 1982.

Taylor,M.J. [82b]: Group laws and rings with normal bases, J. Reine Angew. Math., **337**, 1982, 121–141.

Taylor,M.J. [83]: Relative Galois module structure of rings of integers and elliptic functions, Math. Proc. Cambridge Philos. Soc., **94**, 1983, 389–397; II, Ann. of Math., (2) **121**, 1985, 519–535; III, Proc. London Math. Soc., (3) **51**, 1985, 415–431.

Taylor,M. [84]: *Classgroups of Group Rings*, Cambridge University Press, 1984.

Taylor,M.J. [95]: On the Galois module structure of rings of integers of wild abelian extensions, J. London Math. Soc., (2) **52**, 1995, 73–87.

Taylor,R. [03]: On icosahedral Artin representations, II, Amer. J. Math., **125**, 2003, 549–566.

Teichmüller,O. [36]: Über die Struktur diskret bewerteter Körper, Nachr. Ges. Wiss. Göttingen, 1936, 151–161.

Teichmüller,O. [37]: Diskret bewertete perfekte Körper mit unvollkommenen Restklassenkörper, J. Reine Angew. Math., **176**, 1937, 141–152.

Terada,F. [50]: On a generalization of the principal ideal theorem, Tôhoku Math. J., (2) **1**, 1950, 229–269.

Terada,F. [52]: On the principal genus theorem concerning the abelian extensions, Tôhoku Math. J., (2) **4**, 1952, 141–152.

Terada,F. [53]: A note on the principal genus theorem, Tôhoku Math. J., (2) **5**, 1953, 211–213.

Terada,F. [54a]: Complex multiplication and principal ideal theorem, Tôhoku Math. J., (2) **6**, 1954, 21–25.

Terada,F. [54b]: On the generalized principal ideal theorem, Tôhoku Math. J., (2) **6**, 1954, 95–100.

Terada,F. [55]: A generalization of the principal ideal theorem, J. Math. Soc. Japan, **7**, 1955, 530–536.

Terada,F. [71]: A principal ideal theorem in the genus field, Tôhoku Math. J., (2) **23**, 1971, 697–718.

Thaine,F. [88]: On the ideal class group of real abelian fields, Ann. of Math., (2) **128**, 1988, 1–18.

Thaine,F. [95]: On the p-part of the ideal class group of $Q(\zeta_p+\zeta_p^{-1})$ and Vandiver's conjecture, Michigan J. Math., **42**, 1995, 311–344.

Thérond,J.-D. [95]: Extensions cycliques cubiques monogènes de l'anneau des entiers d'un corps quadratique imaginaire, Archiv Math., **64**, 1995, 216–229.

Thérond,J.-D. [99]: Zyklische kubische monogene Erweiterungen der ganzalgebraischen Zahlen eines quadratischen Körpers, Archiv Math., **72**, 1999, 180–184.

Thomas,E. [79]: Fundamental units for orders in certain cubic number fields, J. Reine Angew. Math., **310**, 1979, 35–55.

Thompson,J.G. [93]: Algebraic integers all of whose conjugates have the same absolute value, in: *Galois Theory, Design Theory, Group Theory*, 107–110. J.Wiley 1993.

Thompson,R.C. [62]: Normal matrices and the normal basis in abelian number fields, Pacific J. Math., **12**, 1962, 1115–1124.

Thompson,W.R. [31]: On the possible forms of discriminants of algebraic fields, Amer. J. Math., **53**, 1931, 81–90; II, **55**, 1933, 111–118.

Thue,A. [12]: Über eine Eigenschaft, die keine transzendente Grösse haben kann, Kr. Vid. Selsk, Skr. I, 191, nr.20. = *Selected Mathematical Papers*, 479–491, Oslo 1977.

Thunder,J.L.,Wolfskill,J. [96]: Algebraic integers of small discriminant, Acta Arith., **75**, 1996, 375–382.

Thurston,H.S. [43]: The solution of p-adic equations, Amer. Math. Monthly, **50**, 1943, 142–148.
Toepken,H. [37]: Zur Irreduzibilität der Kreisteilungsgleichung, Deutsche Math., **2**, 1937, 631–633.
Tollis,E. [97]: Zeros of Dedekind zeta functions in the critical strip, Math. Comp., **66**, 1997, 1295–1321.
Tomanov,G. [88]: On Grunwald-Wang's theorem, J. Reine Angew. Math., **389**, 1988, 209–220.
Torelli,G. [01]: Sulla totalitá dei numeri primi fino ad un limito assegnato, Atti Accad. Napoli, (2) **11**, 1901, 1–215.
Tornheim,L. [55]: Minimal basis and inessential discriminant divisors for a cubic field, Pacific J. Math., **5**, 1955, 623–631.
Touibi,C.,Zargouni,H.S. [89]: Sur le théorème des idéaux premiers, Colloq. Math., **57**, 1989, 157–172.
Toyoizumi,M. [81a]: Formulae for the values of zeta and L-functions at half integers, Tokyo J. Math., **4**, 1981, 193–201.
Toyoizumi,M. [81b]: Ramanujan's formulae for certain Dirichlet series, Comment. Math. Univ. St. Paul, **30**, 1981, 149–173.
Toyoizumi,M. [82]: On the values of the Dedekind zeta function of an imaginary quadratic field at $s = 1/3$, Comment. Math. Univ. St. Paul, **31**, 1982, 159–161.
Tôyama,H. [55]: A note on the different of the composed field, Kōdai Math. Sem. Rep., **7**, 1955, 43–44.
Travesa,A. [90a]: Nombre d'extensions abéliennes sur Q, Sém. Théor. Nombres Bordeaux, (2) **2**, 1990, 413–423.
Travesa,A. [90b]: Generating functions for the number of abelian extensions of a local field, Proc. Amer. Math. Soc., **108**, 1990. 331–339.
Trelina,L.A. [77a]: On algebraic integers with discriminants containing fixed prime divisors, Mat. Zametki, **21**, 1977, 289–296. (Russian)
Trelina,L.A. [77b]: The least prime divisor of an index form, Dokl. Akad. Nauk. Belorus. SSR, **21**, 1977, 975–976. (Russian)
Tsumura,H. [96]: On Demjanenko's matrix and Maillet's determinant for imaginary abelian number fields, J. Number Theory, **60**, 1996, 70–79.
Tsumura,H. [00]: A note on the Demjanenko matrices related to the cyclotomic Z_p-extension, Proc. Japan Acad. Sci., **76**, 2000, 99–103.
Tunnell,J. [81]: Artin's conjecture for representations of octahedral type, Bull. Amer. Math. Soc., (N.S.) **5**, 1981, 173–175.
Turán,P. [50]: On the remainder-term of the prime number formula, II, Acta Math. Acad. Sci. Hungar., **1**, 1950, 155–166.
Turán,P. [53]: *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953. [English translation: J.Wiley 1984].
Turnbull,H.W. [41]: On certain modular determinants, Edinburgh Math. Notes, **32**, 1941, 23–30.
Tzermias,P. [98]: Algebraic points of low degree on the Fermat curve of degree 7, Manuscripta Math., **97**, 1998, 483–488.
Uchida,K. [70]: Unramified extension of quadratic number fields, Tôhoku Math. J., (2) **22**, 1970, 138–141; II, 220–224.
Uchida,K. [71]: Class numbers of imaginary abelian number fields, Tôhoku Math. J., (2) **23**, 1971, 97–104; II, 335–348; III, 573–580.
Uchida,K. [72]: Imaginary abelian number fields with class number one, Tôhoku Math. J., (2) **24**, 1972, 487–499.
Uchida,K. [73]: Relative class numbers of normal CM-fields, Tôhoku Math. J., (2) **25**, 1973, 347–353.

Uchida,K. [74]: Class number of cyclic cubic fields, J. Math. Soc. Japan, **26**, 1974, 447–453.
Uchida,K. [75]: On Artin L-functions, Tôhoku Math. J., (2) **27**, 1975, 75–81.
Uchida,K. [76a]: Isomorphisms of Galois groups, J. Math. Soc. Japan, **28**, 1976, 617–620.
Uchida,K. [76b]: On a cubic field with discriminant 163^2, J. Number Theory, **8**, 1976, 346–349.
Uchida,K. [77a]: Isomorphisms of Galois groups of algebraic number fields, in: *Algebraic Number Theory (Kyoto)*, 263–266. Tokyo 1977.
Uchida,K. [77b]: When is $Z[a]$ the ring of integers? Osaka Math. J., **14**, 1977, 155–157.
Uchida,K. [88]: Imaginary abelian number fields of degrees 2^m with class number one, in: *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata 1986)*, 151–170.
Uchida,K. [94]: On Silverman's estimate of regulators, Tôhoku Math. J., (2) **46**, 1994, 141–145.
Uehara,T. [75]: Vandiver's congruence for the relative class number of an imaginary abelian field, Mem. Fac. Sci. Kyushu Univ., **29**, 1975, 249–254.
Uehara,T. [82]: On some congruences for generalized Bernoulli numbers, Rep. Fac. Sci. Engrg. Saga Univ., **10**, 1982, 1–10.
Uehara,T. [83]: Construction of certain real quadratic fields, Proc. Japan Acad. Sci., **59**, 1983, 390–392.
Ullom,S. [69]: Normal bases in Galois extensions of number fields, Nagoya Math. J., **34**, 1969, 153–167.
Ullom,S. [70]: Ideal normal bases in Galois extensions of number fields, Nagoya Math. J., **39**, 1970, 141–148
Ullom,S. [74a]: Integral representations afforded by ambiguous ideals in some abelian extensions, J. Number Theory, **6**, 1974, 32–49.
Ullom,S. [74b]: The nonvanishing of certain character sums, Proc. Amer. Math. Soc., **45**, 1974, 164–166.
Ullom,S. [76]: A survey of class groups of integral group rings, in *Algebraic Number Fields*, 497–524, Academic Press 1977.
Ullom,S. [80]: Galois module structure for intermediate extensions, J. London Math. Soc., (2) **22**, 1980, 204–214.
Ullom,S. [81]: Ratios of rings of integers as Galois modules, in: *Integral Representations and Applications*, 240–246, Lecture Notes in Math., **882**, Springer 1981.
Urazbaev,B.M. [54]: On an asymptotical formula in algebra, Dokl. Akad. Nauk SSSR, **95**, 1954, 935–938. (Russian)
Urazbaev,B.M. [72]: *Asymptotical Formulas in Algebra*. Alma-Ata 1972. (Russian)
Urbanowicz,J.,Williams,K.S. [00]:: *Congruences for L-functions*, Kluwer 2000.
Urbelis,I. [64]: Distribution of primes in the real quadratic field $K(\sqrt{2})$, Lit. Mat. Sb., **4**, 1964, 409–427. (Russian)
Urbelis,I. [65a]: Distribution of primes in a totally real algebraic number field, Lit. Mat. Sb., **5**, 1965, 307–324. (Russian)
Urbelis,I. [65b]: Distribution of algebraic prime numbers, Lit. Mat. Sb., **5**, 1965, 504–516. (Russian)
Ursell,H.D. [74]: The degrees of radical extensions, Canad. Math. Bull., **17**, 1974, 615–617.
Uzkov,A.I. [63]: On the decomposition of modules over a commutative ring in direct sums of cyclic submodules, Mat. Sb., **62**, 1963, 469–475. (Russian)
Vaaler,J.D.,Voloch,J.F. [00]: The least nonsplit prime in Galois extensions of Q, J. Number Theory, **85**, 2000, 320–335.

Valenza,R.J. [90]: Elasticity of factorization in number fields, J. Number Theory, **38**, 1990, 212–218.

Vámos,P. [70]: The decomposition of finitely generated modules and fractionally self-injective rings, J. London Math. Soc., (2) **16**, 1970, 209–219.

Vandiver,H. [18]: On the first factor of the class number of a cyclotomic field, Bull. Amer. Math. Soc., **25**, 1918/19, 458–461.

Vandiver,H. [20]: On Kummer's memoir of 1857 concerning Fermat last theorem, Proc. Nat. Acad. Sci. U.S.A., **6**, 1920, 266–269; II, Bull. Amer. Math. Soc., **28**, 1922, 400–407.

Vandiver,H. [29a]: On Fermat's last theorem, Trans. Amer. Math. Soc., **31**, 1929, 613–642.

Vandiver,H. [29b]: A theorem of Kummer's concerning the second factor of the class number of a cyclotomic field, Bull. Amer. Math. Soc., **35**, 1929, 333–335.

Vandiver,H. [34]: Fermat's last theorem and the second factor in the cyclotomic class number, Bull. Amer. Math. Soc., **40**, 1934, 118–126.

Vandiver,H. [39a]: On basis systems for groups of ideal classes in a properly irregular cyclotomic field, Proc. Nat. Acad. Sci. U.S.A., **25**, 1939, 586–591.

Vandiver,H. [39b]: On the composition of the group of ideal classes in a properly irregular cyclotomic field, Monatsh. Math. Phys., **48**, 1939, 369–380.

Vandiver,H. [41]: On improperly irregular cyclotomic fields, Proc. Nat. Acad. Sci. U.S.A., **27**, 1941, 77–83.

Värmon,J. [30]: Über die Klassenzahl Abelscher Körper, Ark. Mat., **22**, 1930, no.13, 1–47.

Varnavides,P. [52]: The euclidean real quadratic fields, Indag. Math., **14**, 1952, 111–122.

Vassiliou,P. [32]: Über den Grad eines Primideals in einem komponierten Körper, Rend. Circ. Mat. Palermo, **56**, 1932, 446–448.

Vassiliou,P. [33]: Bestimmung der Führer der Verzweigungskörper relativabelscher Zahlkörper. Beweis der Produktformel für den Führer-Diskriminanten-Satz, J. Reine Angew. Math., **169**, 1933, 131–139.

Veldkamp,G.R. [60]: Remark on Euclidean rings, Nieuw. Tid. Wisk., **48**, 1960/61, 268–270. (Dutch).

Vélez,W.Y. [77]: Prime ideal decomposition in $F(\mu^{1/m})$, II, in: *Number Theory and Algebra*, 331–338, Academic Press 1977.

Vélez,W.Y. [78]: Prime ideal decomposition in $F(\mu^{1/p})$, Pacific J. Math., **75**, 1978, 589–600.

Vel'min,V.P. [51]: Determination of fundamental units and the class-group of cubic fields, Mat. Sb., **5**, 1951, 53–58.

Venkov,A.B.,Proskurin,N.V. [82]: Automorphic functions and Kummer's problem, Uspekhi Mat. Nauk, **37**, 1982, No.3, 143–165. (Russian)

Venkov,B.A. [31]: Über die Klassenzahl positiver binären quadratischen Formen, Math. Z., **33**, 1931, 350–374.

Vignéras,M.F. [74]: Partie fractionnaire de zêta au point -1, C.R. Acad. Sci. Paris, **279**, 1974, 359–361.

Vignéras,M.F. [75a]: Quaternions et applications, Astérisque, **24/25**, 1975, 47–56.

Vignéras,M.F. [75b]: Nombre de classes d'un ordre d'Eichler et valeur au point -1 de fonction zêta d'un corps quadratique réel, Enseign. Math., (2) **21**, 1975, 69–105.

Villegas,F.R. [99]: Modular Mahler measures, I, in; *Topics in Number Theory, (University Park, PA, 1997)*, 17–48, Math. Appl., **467**, Kluwer 1999.

Vijayaraghavan,T. [40]: On the fractional parts of powers of numbers, J. London Math. Soc., **15**, 1940, 159–160; II, Proc. Cambridge Philos. Soc., **37**, 1941, 349–357; III, J. London Math. Soc., **17**, 1942, 137–138; IV, J. Indian Math. Soc., **12**, 1948, 33–39.

Vinberg,E.B. [65]: On the theorem on infinite dimensionality of an associative algebra, Izv. Akad. Nauk SSSR, Ser. Mat., **29**, 1965, 209–214. (Russian)

Vinogradov,A.I. [62]: On the class number, Dokl. Akad. Nauk SSSR, **146**, 1962, 274–276. (Russian)

Vinogradov,A.I. [63a]: On the number of ideal classes and the group of divisor classes, Izv. Akad. Nauk SSSR, Ser. Mat., **27**, 1963, 561–576. (Russian)

Vinogradov,A.I. [63b]: On Siegel's zeros, Dokl. Akad. Nauk SSSR, **151**, 1963, 479–481. (Russian)

Vinogradov,A.I. [64]: Sieve methods in algebraic fields. Lower bounds. Mat. Sb., **64**, 1964, 52–78. (Russian)

Vinogradov,A.I. [65]: On the continuability into the left half-plane of the scalar product of Hecke L-series with Grössencharacters, Izv. Akad. Nauk SSSR, Ser. Mat., **29**, 1965, 485–492. (Russian)

Vinogradov,A.I. [71]: Artin's L-series and the adele groups, Trudy Mat. Inst. Steklov., **112**, 1971, 105–122. (Russian)

Vinogradov,A.I. [73]: Artin's conjectures and reciprocity law, Trudy Mat. Inst. Steklov., **132**, 1973, 35–43. (Russian)

Voloch,J.F. [00]: Chebyshev's method for number fields, J. Théor. Nombres Bordeaux, **12**, 2000, 81–85.

Vorhauer,U.M.A.,Wirsing,E. [01]: On Sarnak's rigidity conjecture, J. Reine Angew. Math., **531**, 2001, 35–47.

Voronin,S.M. [75a]: A theorem on the "universality" of the Riemann zeta-function, Izv. Akad. Nauk SSSR, Ser. Mat., **39**, 1975, 475–486. (Russian)

Voronin,S.M. [75b]: On functional independence of Dirichlet's L-functions, Acta Arith., **27**, 1975, 493–503. (Russian)

Voronoi,G.F. [96]: *On a Generalization of the Continued Fraction Algorithm*,, Warszawa 1896. (Russian)

Voronoi,G. [04]: Sur une propriété du discriminant des fonctions entiéres, in: *Verhandl. III Internat. Kongr.*, 186–189, Heidelberg 1904.

Vostokov,S.V. [74]: Ideals of an Abelian p-extension of an irregular local field as Galois modules, Zap. Nauchn. Sem. LOMI, **46**, 1974, 14–35. (Russian)

Vostokov,S.V. [76a]: Ideals of an Abelian p-extension of a local field as Galois modules, Zap. Nauchn. Sem. LOMI, **57**, 1976, 64–84. (Russian)

Vostokov,S.V. [76b]: A normal basis of an ideal of a local field, Zap. Nauchn. Sem. LOMI, **64**, 1976, 64–68. (Russian)

Vostokov,S.V. [77]: The ring of integral elements of an algebraic number field as a Galois module, Zap. Nauchn. Sem. LOMI, **71**, 1977, 80–84. (Russian)

Voutier,P. [96]: An effective lower bound for the height of algebraic numbers, Acta Arith., **74**, 1996, 81–95.

Vulakh,L.Ya. [02]: Continued fractions associated with $SL_3(Z)$ and units in complex cubic fields, Canad. J. Math., **54**, 2002, 1305–1318.

van der Waal, R.W. [73]: Remarks on the Artin L-functions of the groups $GL_2(F_3)$ and $SL_2(F_3)$, Indag. Math., **35**, 1973, 41–46.

van der Waal, R.W. [74a]: On splitting properties of primes by means of Artin conductors, Indag. Math., **36**, 1974, 82–88; corr. p.411.

van der Waal, R.W. [74b]: A remark on the zeta-function of an algebraic number field, J. Reine Angew. Math., **266**, 1974, 159–162.

van der Waal, R.W. [75]: On a conjecture of Dedekind on zeta-functions, Indag. Math., **37**, 1975, 83–86.

van der Waal, R.W. [82]: Some results connected to Dedekind's zeta functions, Abh. Braunschw. Wiss. Ges., **33**, 1982, 247–251.
van der Waal, R.W.,Sato,K. [93]: On a problem of R.Brauer for quotients of Dedekind zeta-functions, Indag. Math., (N.S.) **4**, 1993, 99–109.
Wada,H. [66]: On the class number and the unit group of certain algebraic number fields, J. Fac. Sci. Univ. Tokyo, **13**, 1966, 201–209.
Wada,H. [70]: On cubic Galois extensions of $Q(\sqrt{-3})$, Proc. Japan Acad. Sci., **46**, 1970, 397–400.
Waerden,B.L. van der [28]: Ein logarithmenfreier Beweis des Dirichletschen Einheitssatzes, Abh. Math. Sem. Univ. Hamburg, **6**, 1928, 259–262.
Waerden,B.L. van der [30]: *Moderne Algebra*, Springer 1930–1931; 3rd ed. 1950. [English translation: Springer 1991.]
Waerden,B.L. van der [34]: Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111**, 1934, 731–733.
Wagner,C. [96]: Class numbers 5,6 and 7, Math. Comp., **65**, 1996, 785–800.
Wagstaff,S.S, [78]: The irregular primes to 125 000, Math. Comp., **32**, 1978, 583–591.
Wahlin,G.E. [15a]: A new development of the theory of algebraic numbers, Trans. Amer. Math. Soc., **16**, 1915, 502–508.
Wahlin,G.E. [15b]: The equation $x^l - A \equiv 0 \pmod{p}$, J. Reine Angew. Math., **145**, 1915, 114–138.
Wahlin,G.E. [16]: On the principal units of an algebraic domain $k(\mathfrak{p}, \alpha)$, Bull. Amer. Math. Soc., **23**, 1916/17, 450–455.
Wahlin,G.E. [22]: The factorization of rational primes in a cubic domain, Amer. J. Math., **44**, 1922, 191–203.
Wahlin,G.E. [32]: The multiplicative representation of the principal units of a relative cyclic field, J. Reine Angew. Math., **167**, 1932, 122–128.
Waldschmidt,M. [81]: Transcendance et exponentielles en plusieurs variables, Invent. math., **63**, 1981, 97–127.
Walfisz,Anna [64]: Über die summatorischen Funktionen einiger Dirichletschen Reihen, II, Acta Arith., **10**, 1964, 71–118.
Walfisz,Arnold [25]: Über das Piltzsche Teilerproblem in algebraischen Zahlkörpern, Math. Z., **22**, 1925, 153–188; II, **26**, 1927, 487–494.
Walfisz,Arnold [26]: On the ideal function of quadratic number fields, Prace Mat.-Fiz., **34**, 1925/26, 35–47. (Polish)
Walfisz,Arnold [36]: Zur additiven Zahlentheorie, II, Math. Z., **40**, 1936, 592–607.
Walfisz,Arnold [42]: On the class-number of binary quadratic forms, Tr. Mat. Inst. Gruz. SSR, **11**, 1942, 57–72, 173–186.
Walter,C.D. [77]: A class number relation in Frobenius extensions of number fields, Mathematika, **24**, 1977, 216–225.
Walter,C.D. [79a]: Brauer's class number relations, Acta Arith., **35**, 1979, 33–40.
Walter,C.D. [79b]: Kuroda's class number relation, Acta Arith., **35**, 1979, 41–51.
Walter,C.D. [80]: Pure fields of degree 9 with class number prime to 3, Ann. Inst. Fourier, **30**, 1980, no.2, 1–15.
Wang,K. [84]: On Maillet's determinant, J. Number Theory, **18**, 1964, 306–312.
Wang,S. [48]: A counterexample to Grunwald's theorem, Ann. of Math., (2) **49**, 1948, 1008–1009.
Wang,S. [50a]: On Grunwald's theorem, Ann. of Math., (2) **51**, 1950, 471–484.
Wang,S. [50b]: An existence theorem for abelian extension over algebraic number fields, Sci. Record, **3**, 1950, 25–27.
Wang,Y. [64]: Estimation and applications of character sums, Shuxue Jinzhan, **7**, 1964, 78–83 (Chinese)

Wańtuła, B. [74]: Problem of Browkin on quadratic fields, Zesz. Nauk. Polit. Śl., **386**, 1974, 173–178.
Warlimont,R. [67]: Eine Bemerkung über Dirichletreihen mit Funktionalgleichung, J. Reine Angew. Math., **228**, 1967, 173–178.
Warlimont,R. [71]: Über die k-ten Mittelwerte der Klassenzahlen primitiven binären quadratischer Formen negativer Diskriminante, Monatsh. Math., **75**, 1971, 173–179.
Warner,S. [89]: *Topological Fields*, North-Holland 1989.
Wasén,R. [74]: On sequences of algebraic numbers in pure extensions of prime degree, Colloq. Math., **30**, 1974, 89–104.
Wasén,R. [76]: Remark on a problem of Schinzel, Acta Arith., **29**, 1976, 425–426.
Wasén,R. [77]: On additive relations between algebraic integers of bounded norms, in: *Journées de théorie additive des nombres*, 153–160, Bordeaux 1977.
Washington,L.C. [74]: On the self-duality of Q_p, Amer. Math. Monthly, **81**, 1974, 369–371.
Washington,L.C. [75]: Class numbers and Z_p-extensions, Math. Ann., **214**, 1975, 177–193.
Washington,L.C. [76a]: Relative integral bases, Proc. Amer. Math. Soc., **56**, 1976, 93–94.
Washington,L.C. [76b]: The class number of the field of 5^nth roots of unity, Proc. Amer. Math. Soc., **61**, 1976, 205–208.
Washington,L.C. [78]: The non-p-part of the class number in a cyclotomic Z_p-extension, Invent. math., **49**, 1978, 87–97.
Washington,L.C. [82]: *Introduction to Cyclotomic Fields*, Springer 1982; 2nd. ed. 1997.
Washington,L.C. [86]: Some remarks on Cohen-Lenstra heuristics, Math. Comp., **47**, 1986, 741–747.
Washington,L.C. [87]: Class numbers of the simplest cubic fields, Math. Comp., **48**, 1987, 371–384.
Washington,L.C. [89]: Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine, in: *Théorie des nombres (Quebec 1987)*, 990–993, de Gruyter 1989.
Washington,L.C.,Zhang X. [97]: Modification of Cohen-Lenstra heuristic for ideal class groups and numbers of certain real quadratic fields, Chinese Sci. Bull., **42**, 1997, 1959–1962.
Watabe,M. [78]: On class numbers of some cyclotomic fields, J. Reine Angew. Math., **301**, 1978, 212–215; corr.: **329**, 1981, p.176.
Watabe,M. [82]: On certain Diophantine equations in algebraic number fields, Proc. Japan Acad. Sci., **58**, 1982, 410–412.
Watabe,M. [83]: On certain cubic fields, I–IV, Proc. Japan Acad. Sci., **59**, 1983, 66–69, 107–108, 260–262, 387–389; V,VI, Proc. Japan Acad. Sci., **60**, 1984, 302–305, 331–332.
Watanabe,S. [92]: An integral basis for a field generated by the lth roots of rational numbers over the rational number field, Tôhoku Math. J., (2) **44**, 1992, 219–231.
Waterhouse,W.C. [70]: The sign of the Gaussian sum, J. Number Theory, **2**, 1970, p.363.
Waterhouse,W.C. [73]: Pieces of eight in class groups of quadratic fields, J. Number Theory, **5**, 1973, 95–97.
Waterhouse,W.C. [76]: Pairs of quadratic forms, Invent. math., **37**, 1976, 157–164.
Waterhouse,W.C. [77]: A nonsymmetric Hasse-Minkowski theorem, Amer. J. Math., **99**, 1977, 755–759.
Waterhouse,W.C. [78]: A probable Hasse principle for pencils of quadrics, Trans. Amer. Math. Soc., **242**, 1978, 297–306.

Waterhouse,W.C. [79]: The normal basis theorem, Amer. Math. Monthly, **86**, 1979, p.212.

Watkins,M. [04a]: Real zeros of real odd Dirichlet L-functions, Math. Comp., **73**, 2004, 415–423.

Watkins,M. [04b]: Class numbers of imaginary quadratic fields, Math. Comp., to appear.

Weber,H[einrich]. [86]: Theorie der Abelscher Zahlkörper, Acta Math., **8**, 1886, 193–263; II, **9**, 1886/87, 105–130.

Weber,H. [96a]: Über einen in der Zahlentheorie angewandten Satz der Integralrechnung, Nachr. Ges. Wiss. Göttingen, 1896, 275–281.

Weber,H. [96b]: *Lehrbuch der Algebra*, vol. II, III, Braunschweig 1896, 1908.

Weber,H. [97]: Über Zahlengruppen in algebraischen Körpern, Math. Ann., **48**, 1897, 433–473; II, **49**, 1897, 83–100; III, **50**, 1898, 1–26.

Weber,H. [05]: Über komplexe Primzahlen in Linearformen, J. Reine Angew. Math., **129**, 1905, 35–62.

Weber,H. [07]: Über zyklische Zahlkörper, J. Reine Angew. Math., **132**, 1907, 167–188.

Weber,H.,Wellstein,J. [13]: Der Minkowskische Satz über die Körperdiskriminante, Math. Ann., **73**, 1913, 275–285.

Weber,H[elmut] [84]: Über die Verteilung ganzer Zahlen mit ausgezeichneten Eigenschaften der Faktorzerlegung in algebraischen Zahlkörpern, Acta Arith., **44**, 1984, 215–239.

Weber,W. [31]: Umkehrbare Ideale, Math. Z., **34**, 1931, 131–157.

Wegner,U. [32a]: Zur Theorie der auflösbaren Gleichung vom Primzahlgrad, I, J. Reine Angew. Math., **168**, 1932, 176–192.

Wegner,U. [32b]: Ein Satz über die Zerlegung von Primzahlen bestimmter arithmetischer Progressionen in algebraischen Zahlkörpern, J. Reine Angew. Math., **168**, 1932, 231–232.

Wegner,U. [35]: Zur Theorie der affektlosen Gleichungen, Math. Ann., **111**, 1935, 738–742.

Weil,A. [36]: Remarques sur des résultats recents de C.Chevalley, C.R. Acad. Sci. Paris, **203**, 1936, 1208–1210 = *Collected Papers*, **I**, 236–240, Springer 1979.

Weil,A. [39]: Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques, Revue Scient., **77**, 1939, 104–106 = *Collected Papers*, **I**, 236–240, Springer 1979.

Weil,A. [43]: Differentiation in algebraic number fields, Bull. Amer. Math. Soc., **49**, 1943, p.41 = *Collected Papers*, **I**, p.329, Springer 1979.

Weil,A. [51]: Sur la théorie de corps de classes, J. Math. Soc. Japan, **3**, 1951, 1–35 = *Collected Papers*, **I**, 483–517, Springer 1979.

Weil,A. [52a]: Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., **73**, 1952, 487–495 = *Collected Papers*, **II**, 63–71, Springer 1979.

Weil,A. [52b]: Sur les "formules explicites" de la théorie des nombres premiers, Medd. Lunds Univ. Math. Sem., 1952, 252–265 = *Collected Papers*, **II**, 48–61, Springer 1979.

Weil,A. [56]: On a certain type of characters of the idèle-class group of an algebraic number field, in: *Proceedings of the International Symposium on Algebraic Number Theory*, 1–7, Tokyo 1956.

Weil,A. [66]: Fonctions zeta et distributions, Sém. Bourbaki, 1966, exp. 312 = *Collected Papers*, **III**, 158–163, Springer 1979.

Weil,A. [67]: *Basic Number Theory*, Springer 1967,

Weil,A. [71]: *Dirichlet Series and Automorphic Forms*, Lecture Notes in Math., **189**, Springer 1979.

Weil,A. [72]: Sur les formules explicites de la théorie des nombres, Izv. Akad. Nauk SSSR, Ser. Mat., **36**, 1972, 3–18 =*Collected Papers*, **III**, 249–264, Springer 1979.
Weil,A. [74]: Sommes de Jacobi et caractéres de Hecke, Nachr. Akad. Wiss. Göttingen, 1974, 1–14 = *Collected Papers*, **III**, 329–342, Springer 1979.
Weinberger,P.J. [69]: A proof of a conjecture of Gauss on class-number two, Ph.D. thesis, Univ. Berkeley 1969.
Weinberger,P.J. [72a]: On euclidean rings of algebraic integers, Proc. Symposia Pure Math., **24**, 1972, 321–332.
Weinberger,P.J. [72b]: A counterexample to the analogue of Artin's conjecture, Proc. Amer. Math. Soc., **35**, 1972, 49–52.
Weinberger,P.J. [73a]: Exponents of the class groups of complex quadratic fields, Acta Arith., **22**, 1973, 117–124.
Weinberger,P.J. [73b]: Real quadratic fields with class numbers divisible by n, J. Number Theory, **5**, 1973, 237–241.
Weinstein,L. [77]: The mean value of the derivative of the Dedekind zeta-function of a real quadratic field, Mathematika, **24**, 1977, 226–236.
Weinstein,L. [79]: The zeros of the Artin L-series of a cubic field on the critical line, J. Number Theory, **11**, 1979, 279–284.
Weinstein,L. [80]: The mean value of the Artin L-series and its derivative of a cubic field, Glasgow Math. J., **21**, 1980, 9–18.
Weisner,L. [28]: Quadratic fields over which cyclotomic polynomials are reducible, Ann. of Math., (2) **29**, 1928, 377–381.
Weiss,A. [83]: The least prime ideal, J. Reine Angew. Math., **338**, 1983, 56–94.
Weiss,A. [96]: *Multiplicative Galois Module Structure*, Amer. Math. Soc. 1996.
Weiss,E. [63]: *Algebraic Number Theory*, New York 1963. [Reprint: Dover 1998.]
Weiss,M.J. [36]: Fundamental systems of units in normal fields, Amer. J. Math., **58**, 1936, 249–254.
Werbiński,T. [88]: An effective version of a theorem of T.Mitsui, Discuss. Math., **9**, 1988, 103–133.
Westlund,J. [03]: On the class number of the cyclotomic number field, Trans. Amer. Math. Soc., **11**, 1910, 388–392.
Westlund,J. [12]: Primitive roots of ideals in algebraic number fields, Math. Ann., **71**, 1912, 246–250.
Westlund,J. [13]: On the factorization of rational primes in cubic cyclotomic fields, Jahresber. Deutsch. Math.-Verein., **22**, 1913, 135–140.
Weyl,H. [40]: *Algebraic Theory of Numbers*, Princeton 1940. [Reprint: Princeton 1998.]
Whitford,E.E. [12]: *The Pell Equation*, New York 1912.
Wieczorkiewicz,J.K. [79]: Some explicit estimates for the Dedekind zeta function, Funct. Approx. Comment. Math., **7**, 1979, 9–12.
Wieczorkiewicz,J.K. [80]: Some remarks on a result of A.V.Sokolovskij, Funct. Approx. Comment. Math., **8**, 1980, 49–58.
Wiegand,R.,Wiegand,S. [77]: Commutative rings whose finitely generated modules are direct sums of cyclics, in: *Abelian Group Theory*, 406–423, Lecture Notes in Math., **616**, Springer 1977.
Wiegandt,R. [59]: On the general theory of Möbius inversion formula and Möbius product, Acta Sci. Math. (Szeged), **20**, 1959, 164–180.
Wiertelak,K. [78]: On the density of certain sets of primes, II, Acta Arith., **34**, 1977/78, 197–210.
Więsław,W. [85]: *Topological Fields*, Marcel Dekker 1985.
Wildanger,K. [00]: Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern, J. Number Theory, **82**, 2000, 188–234.

Wiles,A. [80]: Modular curves and the class group of $Q(\zeta_p)$, Invent. math., **58**, 1980, 1–35.
Wiles,A. [90a]: The Iwasawa conjecture for totally real fields, Ann. of Math., (2) **131**, 1990, 493–540.
Wiles,A. [90b]: On a conjecture of Brumer, Ann. of Math., (2) **131**, 1990, 555–565.
Williams,H.C. [76]: Some results on fundamental units in cubic fields, J. Reine Angew. Math., **286/287**, 1976, 75–85.
Williams,H.C. [80]: Improving the speed of calculating the regulator of certain pure cubic fields, Math. Comp., **35**, 1980, 1423–1434.
Williams,H.C. [81a]: A numerical investigation into the length of the period of the continued fraction expansion of $\sqrt{D}$, Math. Comp., **36**, 1981, 593–601.
Williams,H.C. [81b]: Some results concerning Voronoi's continued fraction over $Q(\sqrt[3]{D})$, Math. Comp., **36**, 1981, 631–652.
Williams,H.C.,Cormack,G.,Seah,E. [80]: Calculation of the regulator of a pure cubic field, Math. Comp., **34**, 1980, 567–611.
Williams,K.S. [70]: Integers of biquadratic fields, Canad. Math. Bull., **13**, 1970, 519–526.
Williams,K.S. [75]: Note on non-Euclidean principal ideal domains, Math. Mag., **48**, 1975, 176–177.
Williams,K.S. [76]: Note on a result of Barrucand and Cohn, J. Reine Angew. Math., **285**, 1976, 218–220.
Williams,K.S. [79]: The class number of $Q(\sqrt{-p})$ modulo 4, for $p \equiv 3 \pmod 4$ a prime, Pacific J. Math., **83**, 1979, 565–570.
Williams,K.S. [81a]: On the class number of $Q(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime, Acta Arith., **39**, 1981, 381–398.
Williams,K.S. [81b]: The class number of $Q(\sqrt{-2p})$ modulo 8, for $p \equiv 5 \pmod 8$ a prime, Rocky Mountain J. Math., **11**, 1981, 19–26.
Williams,K.S. [81c]: The class number of $Q(\sqrt{p})$ modulo 4, for $p \equiv 5 \pmod 8$ a prime, Pacific J. Math., **92**, 1981, 241–248.
Williams,K.S. [82]: Congruences modulo 8 for the class numbers of $Q(\sqrt{\pm p})$, $p \equiv 3 \pmod 4$ a prime, J. Number Theory, **15**, 1982, 182–198.
Williams,K.S. [88]: The class number two problem for certain quartic fields, Congr. Numer., **56**, 1988, 63–70.
Williams,K.S.,Currie,J.D. [82]: Class numbers and biquadratic reciprocity, Canad. J. Math., **34**, 1982, 969–988.
Wilson,N.R. [27]: Integers and basis of a number field, Trans. Amer. Math. Soc., **29**, 1927, 111–126.
Wilson,N.R. [29]: On finding ideals, Ann. of Math., (2) **30**, 1929, 411–428.
Wilson,N.R. [31]: Constructing bases for an algebraic number field, Trans. Roy. Soc. Canada, III, (3) **25**, 1931, 171–184.
Wilson,R.J. [69]: The large sieve in algebraic number fields, Mathematika, **16**, 1969, 189–204.
Wilson,S.M.J. [80]: Extensions with identical wild ramifications, Sém. Th. des Nombres de Bordeaux, **1980/81**, exp.20.
Wilson,S.M.J. [89]: Galois module structure of the rings of integers in wildly ramified extensions, Ann. Inst. Fourier, **39**, 1989, no.3, 529–551.
Wilson,S.M.J. [90]: A projective invariant comparing rings of integers in wildly ramified extensions, J. Reine Angew. Math., **412**, 1990, 35–47.
Wiman,A. [99]: Über die Ideale in einem algebraischen Zahlkörper, nach denen Primitivzahlen existieren, Ofversikt Svenska Vet. Akad. Förhandl., **56**, 1899.
Wingberg,K. [79]: Die Einseinheitengruppe von p-Erweiterungen regulären $\mathfrak{p}$-adischer Zahlkörper als Galoismodul, J. Reine Angew. Math., **305**, 1979, 206–214.

Winter,D.J. [72]: A generalization of the normal basis theorem, Math. Nachr., **54**, 1972, 75–77.
Wintner,A. [45]: The densities of ideal classes and the existence of unities in algebraic number fields, Amer. J. Math., **67**, 1945, 235–238.
Wintner,A. [46a]: The values of the norms in algebraic number fields, Amer. J. Math., **68**, 1946, 223–229.
Wintner,A. [46b]: A factorization of the densities of ideals in algebraic number fields, Amer. J. Math., **68**, 1946, 273–284.
Witt,E. [35]: Über einen Gegenbeispiel zum Normensatz, Math. Z., **39**, 1935, 462–467.
Witt,E. [36]: Zyklische Körper und Algebren der Charakteristik p von Grade p^n, J. Reine Angew. Math., **176**, 1936, 126–140.
Wójcik,J. [69]: On prime ideals with prescribed values of characters of prime degree, Colloq. Math., **20**, 1969, 261–263.
Wójcik,J. [75]: A purely algebraic proof of special cases of Tschebotarev's theorem, Acta Arith., **28**, 1975, 137–145.
Wolfskill,J. [95]: Bounding a unit index in terms of a ring index, Mathematika, **42**, 1995, 199–205.
Wolfskill,J. [97]: Comparing the unit groups of two orders in a number field, Rocky Mountain J. Math., **27**, 1997, 1289–1289.
Wolke,D. [69]: Moments of the number of classes of primitive quadratic forms with negative discriminant, J. Number Theory, **1**, 1969, 502–511.
Wolke,D. [71]: Momente der Klassenzahlen, II, Archiv Math., **22**, 1971, 65–69; III, J. Number Theory, **4**, 1972, 523–531.
Wright,D.J. [89]: Distribution of discriminants of abelian extensions, Proc. London Math. Soc., (3) **58**, 1989, 17–50.
Yager,R.I. [82]: A Kummer criterion for imaginary quadratic fields, Compositio Math., **47**, 1982, 31–42.
Yagi,A. [72]: Explicit formulas for some functions associated with the L-series with some Hecke characters, Bull. Yamagata Univ., **8**, 1972, no.1, 17–27.
Yahagi,O. [78]: Construction of number fields with prescribed l-class groups, Tokyo J. Math., **1**, 1978, 275–283.
Yamagata,S. [76]: A counterexample for the local analogy of a theorem of Iwasawa and Uchida, Proc. Japan Acad. Sci., **52**, 1976, 276–278.
Yamagishi,M. [95]: On the number of Galois p-extensions of a local field, Proc. Amer. Math. Soc., **123**, 1995, 2373–2380.
Yamaguchi,I. [71]: On a property of the irregular class group in a properly irregular l-th cyclotomic field, TRU Math., **7**, 1971, 21–24.
Yamamoto,G. [00]: On the vanishing of Iwasawa invariants of absolutely abelian p-extensions, Acta Arith., **94**, 2000, 365–371.
Yamamoto,K. [58]: Arithmetic linear transformations in an algebraic number field, Mem. Fac. Sci. Kyushu Univ., A, **12**, 1958, 41–66.
Yamamoto,K. [65]: On Gaussian sums with biquadratic residue characters, J. Reine Angew. Math., **219**, 1965, 200–213.
Yamamoto,K. [66]: On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combinat. Th., **1**, 1966, 476–489.
Yamamoto,K.,Onuki,M. [75]: On Kronecker's theorem about Abelian extensions, Sci. Rep. Tokyo Woman's Christian Coll., **35–38**, 1975, 415–418.
Yamamoto,S. [72]: On the rank of the p-divisor class group of Galois extensions of algebraic number fields, Kumamoto J. Sci., **9**, 1972, 33–40.
Yamamoto,Y. [70]: On unramified Galois extensions of quadratic number fields, Osaka Math. J., **7**, 1970, 57–76.

Yamamoto,Y. [71]: Real quadratic number fields with large fundamental units, Osaka Math. J., **8**, 1971, 261–270.
Yamamoto,Y. [84]: Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic, Osaka Math. J., **21**, 1984, 1–22.
Yamamura,K. [91]: A note on class groups of abelian number fields, Proc. Japan Acad. Sci., **67**, 1991, 346–347.
Yamamura,K. [92]: The determination of the imaginary abelian number fields with class number one, Proc. Japan Acad. Sci., **68**, 1992, 21–24; corr. p.74.
Yamamura,K. [94]: The determination of the imaginary abelian number fields with class number one, Math. Comp., **62**, 1994, 899–921.
Yamamura,K. [96]: The maximal unramified extensions of the imaginary quadratic fields with class number two, J. Number Theory, **60**, 1996, 42–50.
Yamamura,K. [97]: Maximal unramified extensions of imaginary quadratic number fields of small conductors, J. Théor. Nombres Bordeaux, **9**, 1997, 405–448.
Yamamura,K. [98]: Determination of the imaginary normal octic number fields with class number one which are not CM-fields, Acta Arith., **86**, 1998, 133–147.
Yang,H.-S., Kwon, S.-H. [99]: The non-normal quartic CM-fields and the octic dihedral CM-fields with relative class number two, J. Number Theory, **79**, 1999, 175–193.
Yin,L. [02]: Stickelberger ideals and divisor class numbers, Math. Z., **239**, 425–440.
Yokoi,H. [60]: On the ring of integers in an algebraic number field as a representation module of Galois group, Nagoya Math. J., **16**, 1960, 83–90.
Yokoi,H. [66]: A cohomological investigation of the discriminant of a normal algebraic number field, Nagoya Math. J., **27**, 1966, 207–211.
Yokoi,H. [67]: On the class number of a relatively cyclic field, Nagoya Math. J., **29**, 1967, 31–44.
Yokoi,H. [68a]: On real quadratic fields containing units with norm -1, Nagoya Math. J., **33**, 1968, 139–152.
Yokoi,H. [68b]: On the divisibility of the class number in an algebraic number field, J. Math. Soc. Japan, **20**, 1968, 411–418.
Yokoi,H. [70a]: On the fundamental unit of real quadratic fields with norm 1, J. Number Theory, **2**, 1970, 106–115.
Yokoi,H. [70b]: Units and class-numbers of real quadratic fields, Nagoya Math. J., **37**, 1970, 61–65.
Yokoi,H. [74]: The diophantine equation $x^3 + dy^3 = 1$ and the fundamental unit of a pure cubic field, $Q(\sqrt[3]{d})$, J. Reine Angew. Math., **268/9**, 1974, 174–179.
Yokoi,H. [86]: Class number one problem for certain kind of real quadratic fields, in: *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata 1986)*, 125–137, Nagoya Univ. 1986.
Yokoi,H. [90]: The fundamental unit and class number one problem of real quadratic fields with prime discriminant, Nagoya Math. J., **120**, 1990, 51–59.
Yokoyama,A. [64]: On the Gaussian sum and the Jacobi sum with its application, Tôhoku Math. J., (2) **16**, 1964, 142–153.
Yokoyama,A. [65]: On class numbers of finite algebraic number fields, Tôhoku Math. J., (2) **17**, 1965, 349–357.
Yokoyama,A. [67]: On the relative class number of finite algebraic number fields, J. Math. Soc. Japan, **19**, 1967, 179–184.
Yoshida,E. [03]: On the 3-class field tower of some biquadratic fields, Acta Arith., **107**, 2003, 327–336.
Yoshida,H. [77]: On Artin L-functions, Japan J. Math., **3**, 1977, 369–380.
Yoshino,K.-I. [97]: A criterion for the parity of the class number of an abelian field with prime power conductor, Nagoya Math. J., **145**, 1997, 163–177.

Yoshino,K.-I. [98]: Class number parity for cyclotomic fields, Proc. Amer. Math. Soc., **126**, 1998, 2589–2591.
Zagier,D. [75a]: A Kronecker limit formula for real quadratic fields, Math. Ann., **213**, 1975, 153–184.
Zagier,D. [75b]: Nombre de classes et fractions continues, Astérisque, **24/25**, 1975, 81–97.
Zagier,D. [76]: On the values at negative integers of the zeta-function of a real quadratic field, Enseign. Math., (2) **22**, 1976, 59–95.
Zagier,D. [77]: Valeurs des fonctions zêta des corps quadratiques réels aux entiers négatifs, Astérisque, **41/42**, 1977, 133–151.
Zagier,D. [81]: *Zetafunktionen und quadratische Körper*, Springer 1981.
Zagier,D. [86]: Hyperbolic manifods and special values of Dedekind zeta-functions, Invent. math., **83**, 1986, 285–301.
Zagier,D. [91]: Polylogarithms, Dedekind zeta function and the algebraic K-theory of fields, in: *Arithmetic Algebraic Geometry (Texel 1989)*, 391–430, Progr. Math., **89**, Birkhäuser 1991.
Zaïmi,T. [94]: Minoration du diamêtre d'un entier algébrique totalement réel, C.R. Acad. Sci. Paris, **319**, 1994, 417–419.
Zaks,A. [76]: Half-factorial domains, Bull. Amer. Math. Soc., **82**, 1976, 721–723.
Zaks,A. [80]: Half-factorial domains, Israel J. Math., **37**, 1980, 281–302. Corr. p.965.
Zanardo,P.,Zannier,U. [91]: The group of Pythagorean triples in number fields, Ann. di Mat. Pura Appl., (4) **159**, 81–88.
Zannier,U. [89]: On the linear independence of roots of unity over finite extensions of Q, Acta Arith., **52**, 1989, 171–182.
Zariski,O.,Samuel,P. [58]: *Commutative Algebra*, New York 1958–60. [Reprint: Springer 1975.]
Zarzycki,P. [91]: Distribution of primes in imaginary quadratic fields in sectors, J. Number Theory, **37**, 1991, 152–160.
Zassenhaus,H. [54]: Über eine Verallgemeinerung des Henselschen Lemmas, Archiv Math., **5**, 1954, 317–325.
Zassenhaus,H. [65]: Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung, in: *Funktionalanalysis, Approximationstheorie, Numerische Mathematik, Oberwolfach 1965*, 90–103, Stuttgart 1965.
Zassenhaus,H. [68]: On a theorem of Kronecker, Delta (Waukesha), **1**, 1968/69, 1–14.
Zassenhaus,H. [72]: On the units of orders, J. Algebra, **20**, 1972, 368–395.
Zaupper,T. [83]: A note on unique factorization in imaginary quadratic fields, Ann. Univ. Sci. Budapest, **26**, 1983, 197–203.
Zaupper,T. [90]: Unique factorization in quadratic number fields, Studia Sci. Math. Hungar., **25**, 1990, 437–445.
Zeinalov,B.A. [65]: Of units of a cyclic real field, Sb. Nauch. Soobshch. Dagestan Univ., 1965, 21–23. (Russian).
Zelinsky,D. [48]: Topological characterization of fields with valuations, Bull. Amer. Math. Soc., **54**, 1948, 1145–1150.
Zelvenskiĭ,I.G. [72]: The algebraic closure of a local field when $p = 2$, Izv. Akad. Nauk SSSR, Ser. Mat., **36**, 1972, 933–946. (Russian)
Zelvenskiĭ,I.G. [78]: The maximal extension without simple ramification of a local field, Izv. Akad. Nauk SSSR, Ser. Mat., **42**, 1978, 1385–1400. (Russian)
Zelvenskiĭ,I.G. [82]: The reduced multiplicative group of a weakly ramified extension of a local field, Zap. Nauchn. Sem. LOMI, **114**, 1982, 131–136. (Russian)
Zhang,M.Y. [95]: On Yokoi's conjecture, Math. Comp., **64**, 1995, 1675–1685.
Zhang,X. [82]: On number fields of type $(2, 2, \ldots, 2)$, J. China Univ. Sci. Tech., **12**, 1982, No.4, 29–41.

Zhang,X. [84a]: Note on a paper of A.A.Albert, J. China Univ, Sci. Tech., **14**, 1984, 171–177.
Zhang,X. [84b]: Density of number fields of type $(2, 2, \ldots, 2)$, Sci. Sinica, **27**, 1984, 345–347.
Zhang,X. [84c]: On number fields of type $(l, l, \ldots, l)$, Sci. Sinica, **27**, 1984, 1018–1026.
Zhang,X. [84d]: Cyclic quartic fields and genus theory of their subfields, J. Number Theory, **18**, 1984, 350–355.
Zhang,X. [84e]: Relative integral bases and units of C_l^n fields, J. Univ. Sci. Techn. China, **14**, 1984, 427–428.
Zhang,X. [85]: A simple construction of genus fields of abelian number fields, Proc. Amer. Math. Soc., **94**, 1985, 393–395.
Zheludevich,F.F. [91]: Local estimates in Lehmer's problem, Acta Arith., **57**, 1991, 225–230.
Zimmer,H.G. [72]: *Computational Problems, Methods and Results in Algebraic Number Theory*, Lecture Notes in Math., **262**, Springer 1972.
Zimmert,R. [81]: Ideale kleiner Normen in Idealklassen und eine Regulatorabschätzung, Invent. math., **62**, 1980/81, 367–380.
Zink,E.W. [75]: Zum Hauptidealsatz von Tannaka-Terada, Math. Nachr., **67**, 1975, 317–325.
Zlebov,E.D, [66]: The Pisot-Vijayaraghavan numbers and fundamental units of algebraic fields, Izv. Akad. Nauk BSSR, 1966, 110–112. (Russian)
Zolotarev,E. [69]: *On an indeterminate cubic equation*, Dissertation, St. Petersburg 1869. (Russian)
Zolotarev,E. [74]: Théorie des nombres entiers complexes avec une application au calcul intégral, Bull. Acad. Sci. St.Petersburg, 1874.
Zolotarev,E. [80]: Sur la théorie des nombres complexes, J. math. pures appl., (3) **6**, 1880, 51–84.
Żyliński,E. [13]: Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper, Math. Ann., **73**, 1913, 273–274.

Author Index

Abrashkin,V.A., 468
Acciaro,V., 189
Adachi,N., 40, 464, 465
Agou,S., 191
Ahern,P.R., 400
Albert,A.A., 77, 78, 252
Albis-Gonzalez,V.S., 308
Albu,T., 79, 119
Allen,S., 509
Amano,K., 308
Amano,S., 252
Amara,H., 125
Amara,M., 75
Amberg,E.J., 78
Amice,Y., 405
Amoroso,F., 74, 75
Anderson,D.D., 507
Anderson,D.F., 507–509
Anderson,G.W., 391
Anferteva,E.A., 122
Angell,L.O., 77
Ankeny,N.C., 82, 124, 402, 403, 459, 462–464, 475, 478
Antoniadis,J.A., 468
Aoki,N., 391
Appelgate,H., 125
Arai,H., 77
Aramata,H., 393, 531
Archinard,G., 39, 80
Armitage,J.V., 126, 188, 311, 397, 476, 530, 532
Arnaudon,M., 308
Arndt,F., 186, 475
Arno,S., 469
Arpaia,P.J., 130
Artin,E., 21, 39, 70, 120–122, 124, 126, 186, 194, 310, 392, 393, 403, 404, 459, 462, 531
Arutyunyan,Z., 254
Arwin,A., 125
Asano,K., 39
Avanesov,E.T., 123, 125
Ax,J., 71, 311
Ayoub,C.W., 308
Ayoub,R.G., 400–402, 468, 481
Azizi,A., 194, 477
Azuhata,T., 123, 479, 480, 532

Baayen,P.C., 507
Babaev,G., 399
Babaitsev,V.A., 466
Bachman,G., 191
Bachmann,P., 122
Bae,S.H., 393
Baily,A.M., 78, 459, 460, 530
Baker,A., 468, 478, 527, 532
Balakrishnan,U., 396
Baldisseri,N., 130
Ballieu,R., 186
Barban,M.B., 399, 474
Barkan,P., 309, 461
Barner,K., 309, 392, 399
Barrucand,P., 192, 195, 389, 394, 479, 480
Barsky,D., 405, 466
Bartels,H.J., 70, 308
Bartz,K., 395, 396
Bass,H., 39, 121, 122
Bateman,P.T., 76
Bauer,H., 476, 479
Bauer,M., 79, 185, 186, 190, 192, 251, 252, 307, 403
Bayad,A., 193
Bayer,P., 252, 399
Bazylewicz,A., 71, 73
Beaumont,R.A., 81
Beeger,N.G.W.H., 460
Behnke,H., 71
Behrbohm,H., 481
Belabas,K., 77, 476, 479
Belcher,P., 530
Benjamin,E., 194, 195

Bennett,A.A., 121
Benson,C.T., 123
Bérczes,A., 79
Berg,E., 130
Bergé,A.M., 78, 129, 189, 253
Berger,R.I., 480
Berger,T.R., 186
Bergmann,G., 69, 125
Bergström,H., 77, 309, 461
Berndt,B.C., 309, 397, 402, 461
Bernstein,L., 123, 125
Bertin,M.J., 76
Bertrandias,F., 189, 253, 311
Bertrandias,J.P., 253
Berwick,W.E.H., 77, 78, 125, 126
Besicovitch,A.S., 404
Bessassi,S., 471
Bessis,J.D., 72
Beukers,F., 128
Bhandari,S.K., 121
Bhaskaran,M., 192
Bickmore,C.F., 124
Bilhan,M., 403, 406
Billevich,K.K., 125
Birch,B.J., 80, 307, 468, 530
Bird,R.F., 404
Biró,A., 472
Bitimbaev,T.S., 461
Blanksby,P.E., 72–74, 76, 82
Blasius,D., 391
Bley,W., 189, 193
Bloom,J.R., 466, 467
Bolling,R., 461
Bombieri,E., 128
Bond,R.J., 194
Borchardt,K.W., 80
Borel,A., 195, 399
Borevich,Z.I., 70, 120, 194, 253, 254, 473
Bosma,W., 481
Bourbaki,N., 39
Boutteaux,G., 471
Bouvier,L., 126, 480
Boyd,D.W., 74–76, 478, 532
Brandal,W., 39
Brandis,A., 123
Brattström,G., 391
Brauer,R., 185, 392, 393, 467, 475, 481, 531
Bredikhin,B.M., 400
Bremner,A., 80, 307, 534
Brentjes,A.J., 125
Breusch,R., 73, 529
Briggs,W.E., 478
Brillhart,J., 403
Brink,J.R., 195
Brinkhuis,J., 187, 189, 190
Browkin,J., 195, 532
Brown,E., 124, 470, 479
Brown,K.S., 399, 465
Brown,M.L., 123
Bruckner,G., 191
Bruegeman,S., 79, 310
Brumer,A., 82, 126, 195, 311, 477, 480
Brunotte,H., 75, 125, 126, 533
Buchmann,J., 78, 192
Buell,D.A., 469, 470
Bugeaud,Y., 70, 75, 128
Buhler,J.P., 393, 465, 466, 469
Bullig,G., 125
Bulota,K., 396, 402
Bumby,R.T., 509
Bundschuh,P., 453, 468
Burns,D.J., 126, 189, 253
Bushnell,C.J., 187, 195, 393
Büsser,A.H., 191
Butts,H.S., 38, 473, 509
Buzzard,K., 393
Byeon,D., 122, 466, 479, 481
Byott,N.P., 189

Cahen,P.J., 508
Callahan,T., 76, 82, 480
Callial,P.F., 397
Calloway,J., 81
Cameron,P.J., 390
Camion,P., 40
Canals,I., 77
Candiotti,A., 466
Cantor,D.G., 72, 74, 127, 308, 311
Carayol,H., 195
Carlitz,L., 185, 190, 459, 462, 479, 485, 507
Carroll,J.E., 466
Carter,D., 121
Carter,J.E., 404
Cassels,J.W.S., 70, 73, 81, 121, 186, 191, 199, 251, 254, 307, 459
Cassou-Noguès,P., 389, 399, 405
Cassou-Noguès,Ph., 187, 189, 193, 195
Castela,C., 481
Cavallar,S., 131
Cerri,J.P., 131
Chabauty,C., 127, 129
Chabert,J.L., 508
Chamizo,F., 474

Chan,S.P., 189, 253
Chandrasekharan,K., 395, 397, 402
Chang,K.Y., 470, 471, 478
Chang,M.L., 80
Chang,S.M., 194
Chao Ko, 130
Chao,N.L., 250
Chapman,R.J., 186
Chapman,S.T., 507–509, 531
Chase,S.U., 39
Chatelain,D., 189
Châtelet,A., 77, 121
Chatland,H., 116, 130
Chebotarev,N.G., 120, 186, 190, 307–309, 403, 404
Chebyshev,P.L., 399, 447
Chen,Y.M.J., 128
Cherubini,J.M., 468
Chevalley,C., 39, 70, 97, 122, 186, 192, 310
Childs,L.N., 187, 189, 193
Chinburg,T., 72, 126, 188, 190, 393
Chowla,P., 397, 479, 481
Chowla,S., 121, 124, 128, 130, 186, 192, 309, 397, 462–464, 467, 468, 472, 473, 475, 477–479, 481, 533
Christofferson,S., 122
Chudakov,N.G., 122, 467, 468
Chulanovskii,I.V., 402
Cioffari,V.G., 130
Claborn,L., 39, 40, 507
Clark,D.A., 117, 131
Coates,J., 127, 193, 399, 465, 468, 477
Cohen,G.L., 400, 402
Cohen,H., 70, 77, 79, 81, 121, 123, 192, 195, 399, 460, 476
Cohen,I.S., 38
Cohn,H., 70, 77, 125, 195, 389, 464, 476, 479, 480
Cohn,J.H.E., 130
Coleman,M.D., 396, 401, 402
Coleman,R.F., 391
Colliot-Thélène,J.L., 308
Colmez,P., 405
Connell,I.G., 480, 481
Conner,P.E., 71
Conrad,M., 187
Conrey,J.B., 395–397, 469, 474
Conway.J.H., 128
Cooke,G.E., 121, 127, 131, 195, 479
Coolidge,J.L., 71
Coray,D., 308
Corbalan,A.G., 71
Cormack,G., 125
Cornacchia,P., 462, 464
Cornell,G., 121, 193, 195, 464, 477, 480
Corput,J.G.van der, 402
Costa,A., 129, 476, 479
Cougnard,J., 80, 187–190, 195, 196
Cowles,M.J., 192, 478
Coykendall,J., 71, 390, 507, 531
Craig,M., 476
Crandall,R., 465, 466
Cremona,J.E., 194
Cresse,G.H., 473
Cucker,F., 71
Cuoco,A.A., 466, 467
Currie,J.D., 479
Cusick,T.W., 125, 129
Cvetkov,V.M., 185
Czarnowski, 397
Czogała,A., 507, 509

Daberkow,M., 81, 195
Dade,E.C., 127, 509
Dalen,K., 185, 251
Damey,P., 480
Daniel,S., 479
Datskovsky,B.A., 77, 460, 474
Davenport,H., 77, 116, 122, 130, 309, 460, 489, 530, 531
David,P., 254
David,S., 75
Davis,H.T., 462
Davis,R.W., 461
Decomps-Guilloux,A., 76, 311
Dedekind,R., 37, 38, 64, 69, 70, 76, 81, 118–121, 132, 167, 185, 186, 190, 191, 389, 393, 401, 460, 473
Degen,C.F., 124
Degert,G., 123
Del Corso,I., 120, 190, 460, 531
Delange,H., 313, 525
Delaunay,B.N., 71, 77, 122, 125, 126, 309
Deligne,P., 391, 393, 398, 405
Delorme,C., 507
Delsarte,S., 420, 459
Dénes,P., 125, 192, 193, 464
Deninger,C., 76
Desnoux,P.J., 479
Deuring,M., 187, 195, 391, 403, 461, 468
Di Franco,F., 507
Diaz y Diaz,F., 78, 79, 81, 82, 121, 195, 460, 476

Dickinson,M., 393
Dickson,L.E., 69, 123, 130, 461, 473
Diekert,V., 251
Dinghas,A., 71
Dirichlet,P.G., 69, 96, 122, 308, 389, 395, 399, 461, 479, 480, 482
Disse,A., 252
Dobrowolski,E., 49, 73, 75
Dodson,M., 125
Dohmae,K., 127, 462, 472, 477
Drakokhrust,Ya.A. , 308
Draxl,P.K.J., 192
Dress,A., 133, 191, 308, 533
Dribin,D.M., 308
Drinfeld,V.G., 310
Dubickas,A., 72–76
Dubois,D.W., 131
Dubois,E., 472, 481
Dujčev,J., 191
Duke,W., 396
Dumitrescu,T., 38
Dummit,D.S., 80
Dürbaum,H., 250
Duval,D., 126
Dvornicich,R., 75, 190, 460, 531
Dwork,B., 393
Dzhiemuratov,U., 402

Eakin,P., 40
Earnest,A.G., 478
Eda,Y., 77, 400, 402
Edgar,H., 78, 404
Edgorov,Zh., 389
Edwards,H.M., 69, 119, 120
Egami,S., 122, 130, 308
Eichler,M., 70, 195, 461
Eie,M., 399
Einsiedler,M., 76
Eisenstein,G.H., 69, 121, 389
Elder,G.G., 253
Elliott,P.T.D.A., 404
Ellison,W., 468
Elstrodt,J., 186
Emde Boas,P.van, 507
Endô,A., 125, 462, 476, 479, 480
Engstrom,H.T., 190
Ennola,V., 72, 77, 128, 129, 481, 529
Epstein,P., 124
Erdős,P., 128, 130, 397, 402
Erez,B., 311
Ernvall,R., 465, 466
Esmonde,J., 70
Estermann,T., 467
Estes,D.R., 464, 478
Euler,L., 69, 185, 398, 478
Evans,R.J., 309, 461
Everest,G.R., 76, 187
Evertse,J.H., 70, 79, 128

Faddeev,D.K., 71, 77, 121, 122, 125, 126, 252
Fainleib,A.S., 474
Fanta,E., 399, 400
Farhane,A., 481
Favard,J., 76
Feit,W., 252
Fekete,M., 71, 72
Feldman,N.I., 468
Feng,K., 127, 404, 462, 480, 507, 510
Ferguson,L.B.O., 72
Ferrero,B., 466
Ferton,M.J., 253
Fesenko,I.B., 199, 254
Fieker,C., 189, 195
Flammang,V., 72, 74–76
Flanders,H., 70, 120, 403
Fleckinger,B., 195, 196
Fleischer,I., 250
Flynn,E.V., 534
Fogels,E., 396, 397, 399–401, 508
Foote,R., 194, 393
Ford,D., 78, 81
Forman,W., 400
Fossum,R.M., 38–40
Foster,L.L.T., 79
Fouvry,E., 479
Fox,G.J., 475
Fraenkel,A., 37, 250
Frei,G., 125
Freiman,G., 509
Fresnel,J., 389, 399, 405
Frey,G., 120, 121, 251, 480
Friedlander,J.B., 396, 399, 400, 468, 472
Friedman,E., 129, 398, 467
Frobenius,G., 375, 403, 452, 481
Fröhlich,A., 70, 121, 126, 187–189, 191–193, 211, 251, 254, 292, 295, 311, 393, 404, 459, 464, 475–478, 480, 530–532
Fryska,T., 396, 397
Fuchs,L., 119, 460
Fuchs,L. (XX ct.), 77
Fuchs,P., 462
Fueter,R., 127, 195, 310, 460
Fujii,A., 397

Fujisaki,G., 252, 404
Fujita,H., 82
Fujiwara,M., 307
Fukuda,T., 466
Funakura,T., 78, 80, 309
Fung,G., 77, 125, 461
Furtwängler,Ph., 182, 185, 192, 194, 307, 399, 400, 463
Furuta,Y., 191, 193, 195, 311, 480
Furuya,H., 193, 194, 480

Gaál,I., 79, 80, 190, 531
Galkin,V.M., 462
Gao,W., 507, 509
Garbanati,D.A., 70, 126, 132, 193, 308, 532
Gassmann,F., 390, 403
Gathen,J.von zur, 191
Gauss,C.F., 39, 69, 120, 122, 130, 186, 190–192, 309, 436, 443, 467, 472, 474, 475, 478, 479, 531
Gauthier,F., 191
Gelbart,S., 195, 392, 393
Gelfond,A.O., 395, 473
Gérardin,P., 392
Gerlovin,E.L., 254
Geroldinger,A., 507–509
Geronimo,J.S., 72
Gerst,I., 403, 404
Gerth,F.III, 121, 193–195, 308, 464, 466, 467, 470, 477, 479, 480
Gethner,E., 533
Geyer,D., 120, 121, 196, 251, 480
Ghate,E., 309
Ghosh,A., 395, 396
Gilbarg,D., 253
Gillard,R., 126, 127, 311, 467
Gilmer,R.W.Jr., 38, 39, 308
Giorgiutti,J., 39
Girstmair,K., 71, 77, 187, 189, 462, 463
Glaisher,J.W.L., 479
Glesser,P., 75
Godin,M., 404
Godwin,H.J., 78, 125, 480
Gogia,S.K., 195, 475
Gold,R., 195, 307, 308, 467, 475, 480
Goldfeld,D., 394, 397, 467, 468
Goldstein,L.J., 70, 398, 400, 404, 460, 461, 463, 470
Golod,E.S., 82, 194
Gomez Ayala,E.J., 187, 195, 196
Gonek,S.M., 396
Gonzalez,N., 508
Good,A., 402
Gordon,B., 533
Gordover,G., 474
Gorenstein,D., 390
Goss,D., 310
Gouvêa,F.Q., 199, 251
Grams,A., 40
Grandcolas,M., 76
Grandet-Hugot,M., 76, 311
Grandjot,K., 186
Grant,D., 128
Granville,A.J., 399, 461, 463, 469, 481
Gras,G., 70, 127, 193–195, 254, 308, 311, 475, 477, 479–481, 531
Gras,M.N., 80, 477, 480
Greaves,A., 72
Grebenyuk,D.G., 78
Greenberg,M.J., 309
Greenberg,R., 127, 397, 465–467
Greiter,G., 71, 125
Greither,C., 126, 187, 189, 196, 476, 480
Grell,H., 39, 185
Gronwall,T.H., 468
Gross,B.H., 391, 468, 469
Grossman,E.H., 129
Grosswald,E., 468, 478
Grotz,W., 402
Grube,F., 478
Gruenberg,K.W., 194
Grundman,H.G., 125
Grunewald,F., 186
Grunwald,W., 310
Guého,M.F., 399
Guerrier,W.J., 186
Gundlach,K.-B., 399
Gupta,H., 131
Gurak,S., 127, 308
Guralnick,R.M., 71
Gurevich,M.M., 311
Gut,M., 120, 191, 195, 460, 465, 479, 480
Güting,R., 125
Guy,M.J.T., 307
Győry,K., 70, 71, 79, 80, 125, 128, 129, 529, 530, 532

Haberland,K., 460
Hachami,S., 480
Haddad,N., 81
Hafner,J.L., 402
Haggenmüller,R., 124
Hajir,F., 82, 186, 194, 195

Halbritter,U., 399
Hall,N.A., 478
Hall,R.R., 402
Halter-Koch,F., 72, 125, 126, 130, 185, 187, 191, 252, 254, 308, 404, 472, 475–477, 480, 481, 507–510
Hamada,S., 308
Hamamura,M., 478
Haneke,W., 467, 481
Happle,W., 481
Hara,Y., 398
Haran,S., 392
Harder,G., 465
Hardy,G.H., 76, 191, 395
Hardy,K., 78, 460, 470, 479
Harris,M., 195
Hartung,P., 397, 479
Haselgrove,C.B, 397
Hasse,H., 70, 77, 79, 97, 118, 121, 123, 125–127, 132, 191, 192, 194, 195, 250, 252, 307–310, 390–393, 402, 403, 459–462, 464, 475, 476, 479, 530, 532
Hassler,W., 507
Haugland,J.K., 533
Hayashi,H., 479
Hayashi,Y., 480
Hayes,D.R., 310, 398
Hays,J.H., 38
Hazama,F., 462
Hazewinkel,M., 254
Heath-Brown,D.R., 309, 396, 478, 532
Hecke,E., 70, 119, 185, 186, 192, 195, 292, 306, 309–311, 316, 330, 389, 395, 397, 398, 400, 402, 404, 406, 432, 460, 461, 467, 473, 480
Heegner,K., 468
Heider,F.P., 194, 307, 308
Heilbronn,H., 77, 116, 130, 392, 397, 460, 467, 468, 530, 531
Heinzer,W., 40
Hendy,M.D., 478, 481
Henniart,G.M., 195
Hensel,K., 65, 79, 120, 185, 186, 190–192, 250–252, 255, 307, 308
Hensley,D., 402
Herbrand,J., 120, 126, 185, 192, 194, 308, 463, 465
Herglotz,G., 398
Hermite,C., 52, 68, 80, 81, 122, 125
Herr,J., 509
Herz,C.S., 195, 475
Heß,F., 309
Hewitt,E., 511, 514
Hida,H., 399
Higman,G., 190
Hijikata,H., 308
Hilano,T., 396
Hilbert,D., 38, 70, 119, 120, 127, 186, 187, 191, 193–195, 253, 263, 307–309, 404, 459
Hinz,J., 308, 396, 397, 399–401, 534
Hirabayashi,M., 462
Hiramatsu,T., 192
Hirzebruch,F., 399, 481
Hock,A., 453, 468
Hodges,W., 38
Hoffstein,J., 389, 463, 470–473
Hofreiter,N., 130
Holland,D., 126, 189
Holtz,N.M., 78, 460
Holzer,L., 480
Honda,T., 464, 479, 480, 482
Hooley,C., 124, 474
Hooper,J., 189
Horie,K., 123, 193, 464, 466, 470, 477, 479, 481
Horie,M., 308, 470, 475
Hua,L.K., 130, 473
Huard,J.G., 78, 459
Huckaba,J.A., 38
Hudson,R.H., 78, 460, 461, 470
Hughes,J., 126, 532
Humbert,P., 478
Hunter,J., 71, 76, 81
Hürlimann,W., 71
Hurrelbrink,J., 476
Hurwitz,A., 120, 121, 389, 398, 403, 479
Hutchinson,K., 71, 404
Huxley,M.N., 401
Hwang,H.J., 481
Hymo,J.A., 404
Hyyrö,S., 462

Ichimura,H., 80, 187, 466, 479, 480, 532
Idelhadj,A., 38
Iimura,K., 121, 125, 193, 480
Ikeda,M., 196
Inaba,E., 251, 464, 476, 480
Indlekofer,K.H., 81
Inkeri,K., 462
Ireland,K.F., 70
Irfan,M., 38
Iseki,K., 402
Ishibashi,M., 481
Ishida,M., 125, 393, 475, 480
Ishikawa,M., 128

Iskovskikh,V.A., 307
Ito,H., 191, 309
Itoh,T., 187
Iwaniec,H., 396, 469, 474
Iwasaki,K., 459
Iwasawa,K., 122, 123, 192–194, 196, 251, 254, 310, 311, 390, 391, 405, 461, 464, 466, 477, 480
Iwata,H., 251
Iyanaga,S., 70, 194, 475

Jacobi,C.G.J., 69, 125, 391, 482
Jacobinski,H., 189
Jacobson,B., 530
Jacobson,E., 310, 390
Jacobson,M.J.Jr., 476
Jacobsthal,E., 127
Jakubec,S., 124, 189, 464
Janssen,U., 251
Janusz,G., 70
Járási,I., 79, 80
Jarden,M., 251, 403
Jaulent,J.F., 126, 187, 189, 193, 194, 481
Jehne,W., 194, 307, 308, 394, 403, 404, 467, 481, 532
Jenkner,W., 251
Jensen,C.U., 38, 76, 124, 391
Jensen,K.L., 465
Jha,V., 461
Ji,C., 187
Johnson,D., 396
Johnson,D.H., 131
Jones,A.J., 128
Jones,B.W., 473
Jones,J.W., 79, 310
Jordan,J.H., 399, 533
Joris,H., 402
Jung,S.W., 470
Jutila,M., 396, 474

Kable,A.C., 80
Kaczorowski,J., 395, 400, 486, 507–509, 531
Kagawa,T., 308
Kallies,J., 399
Kambayashi,T., 252
Kanemitsu,S., 402, 462, 473
Kanno,T., 196
Kaplan,P., 126, 195, 476, 479
Kaplansky,I., 39, 250
Karatsuba,A.A., 401
Kátai,I., 81
Kataoka,T., 186
Katayama,K., 398, 399
Katayama,S., 472, 474
Katayama,S.I., 472
Kaufman,R.M., 395, 396, 402
Kawada,Y., 186, 252
Kawamoto,F., 187, 196, 253
Keating,M., 187
Keller,G., 121
Kemp,P., 472
Kempfert,H., 194
Kenku,M.A., 468
Kennedy,R.E., 39
Kersey,D., 127
Kessler,I., 533
Khare,C., 465
Kida,Y., 467
Kim,H.K., 472, 481
Kim,J.M., 466
Kim,S., 189
Kiming,I., 393
Kimura,N., 479
Kimura,T., 193, 464, 477
King,H., 461
Kinohara,A., 186
Kiselev,A.A., 461, 462, 479
Kishi,Y., 479, 480
Kisilevsky,H., 80, 194, 195, 466, 467, 476, 478
Kitaoka,Y., 128
Kleboth,H., 465
Kleiman,H., 251
Klingen,H., 398
Klingen,N., 390, 404
Knapowski,S., 402, 467
Knebusch,M., 311
Kneser,H., 71
Kneser,M., 404
Knuth,D.E., 191
Kobayashi,M., 310
Kobayashi,S., 193, 477, 480
Koblitz,N., 199, 251, 405
Koch,H., 70, 120, 194, 196, 252, 392, 479
Kohnen,W., 479
Kolyvagin,V.A., 127, 465
Komatsu,K., 79, 196, 310, 311, 390, 404, 466, 479
Komatsu,T., 193
König,R., 473
Konno,S., 398
Konyagin,S.V., 75
Koppenhöfer,D., 80

Korchagina,V.I., 402
Körner,O.H., 478
Kőrnyei,I., 81
Koshi,Y., 480
Kostra,J., 82, 129, 189
Kostrikin,A.J., 194
Kovács,B., 81
Kovalchik,F.B., 402
Kowalsky,H.J., 250
Koyama,T., 38
Kraft,J.S., 466, 467
Krakowski,F., 120
Kramer,D., 399
Krasner,M., 195, 251–254, 308
Krause,U., 507, 510
Kronecker,L., 49, 71, 81, 119–122, 132, 186, 190, 309, 310, 375, 398, 403, 425, 461, 464, 475
Krull,W., 38, 39, 81, 120
Kruyswijk,D., 507
Kubert,D.S., 127, 391, 460, 464
Kubilius,I.P., 402
Kubota,K.K., 530
Kubota,T., 125, 196, 309, 405, 459, 480
Kubotera,N., 466
Kučera,R., 127, 462, 480
Kudo,A., 465, 479, 480
Kühnova,J., 462
Kulkarni,R.S., 77
Kummer,E.E., 39, 69, 119–121, 125–127, 167, 190, 191, 193, 309, 425, 460–465
Kunert,D., 309
Kuniyoshi,H., 194
Kurihara,M., 465
Kuroda,S., 125, 191, 480, 481
Kuroda,S.N., 122, 186, 191, 193, 476–478
Kurokawa,N., 392
Kürschak,J., 39, 120, 250, 251
Kutsuna,M., 124, 481
Kuzmin,L.V., 127, 194, 311
Kuzumaki,T., 462
Kwon,S.H., 78, 82, 470, 471, 478

Labesse,J.P., 392
Lachaud,G., 472
Lafon,J.P., 39
Lagarias,J.C., 124, 127, 394, 401, 403, 476, 530
Lagrange,J.L., 120, 121, 123, 309
Lai,D.T., 402
Lakein,R.B., 122
Lakkis,K., 393, 394
Lamprecht,E., 195, 309
Lánczi,E., 192
Landau,E., 70, 81, 120, 129, 143, 185, 186, 389, 395–397, 399–402, 461, 467, 468, 473
Landherr,W., 308
Landsberg,G., 78
Lang,H., 124, 398, 399, 464, 479, 481
Lang,S., 70, 127, 128, 193, 389, 392, 399, 402, 459, 460, 465
Lang,S.D., 464
Langevin,M., 75, 76
Langlands,R.M., 392, 393
Lardon,R., 508
Larsen,M.D., 38, 39
Lasker,E., 38, 185
Latham,J., 532
Latimer,C.G., 121, 125, 126, 191, 464
Lau,C.F., 72
Laubie,F., 192
Laumon,G., 195
Laurinčikas,A., 390
Lavrik,A.F., 130, 389, 395, 474
Lawton,W., 75
Le,M.H., 389, 473
Lebesgue,V.A., 186
Ledermann,W., 78
Lednev,N.A., 126
Lee,K.C., 399
Lee,Y., 476
Leedham-Green,C.R., 40
Leep,D.B., 308
Lefeuvre,Y., 471
Legendre,A.M., 124
Lehmer,D.H., 71–73, 124, 462, 468, 529
Lemmermeyer,F., 69, 122, 130, 131, 193, 195, 465, 471, 481
Lemmlein,V.G., 131
Lenstra,H.W.Jr., 127, 129, 131, 308, 403, 476, 532, 534
Leon,M.J.de, 397
Leonard,P.A., 479
Leopoldt,H.W., 78, 189, 252, 253, 309, 311, 405, 460, 475, 476, 480, 531
Lepistö,T., 462, 463, 467, 470
Lequain,Y., 38
Lerch,M., 461, 468, 479
Letard,P., 81
Lettl,G., 189, 253, 477, 507, 509
Leu,M.G., 472
Leutbecher,A., 131
Levesque,C., 125, 472

Levi,F., 186
Levin,B.V., 399
Levy,L.S., 40
Lewin,J., 81
Lewis,D.J., 128, 403, 530
Lewittes,J., 309
Li,H.C., 254
Liang,J.J., 80, 81, 186, 195, 251
Liardet,P., 530
Lichtenbaum,S., 391, 399
Lidl,R., 191
Lienen,H.v., 124
Lim,C.H., 189, 253
Lind,D., 76
Linden,F.J.van der, 130, 131
Linfoot,E., 468
Linnik,J.V., 402, 467, 473
Lippmann,R.A., 478
Littlewood,J.E., 395, 473
Litver,E.L., 78, 480
Livingston,M., 533
Llorente,P., 77, 79, 125, 191, 476
Lloyd-Smith,C.W., 75, 76
Lochter,M., 390, 404, 532
Lodemann,M., 397, 401
Long,R.L., 70, 404
Lorenz,F., 187, 308
Louboutin,R., 74
Louboutin,S., 122, 389, 397, 461, 470–473, 478, 481
Low,M., 397
Loxton,J.H., 72, 82, 129, 309, 389
Lu,H.W., 472, 481
Lubelski,S., 81, 122, 309, 473
Lubin,J., 254
Lukes,R.F., 476
Lundström,P., 459
Luthar,I.S., 77, 195, 402, 475

Macaulay,F.S., 38
MacCluer,C.R., 125, 192, 403
MacKenzie,R.E., 252
MacKenzie,R.M., 404
Mac Lane,S., 120, 250
Madan,M.L., 253, 478, 480
Madden,D.J., 195
Magnus,W., 194
Mahler,K., 77, 121, 122, 128, 129, 199, 251, 468, 473
Maillot,V., 76
Maire,C., 82, 186, 194
Mäki,S., 125, 459, 460
Maknis,M., 396, 401, 402
Mallik,A., 475, 481
Man,S.H., 38
Manin,Yu.I., 307
Mann,H.B., 40, 70, 77, 128, 185, 191, 403, 404
Marcus,D.A., 70
Marko,F., 126
Marszałek,R., 254
Martel,B., 253
Martinet,J., 77, 78, 81, 82, 129, 131, 187–191, 194, 392, 393, 404, 476, 480
Masley,J.M., 462, 463, 470, 481
Massy,R., 252, 404
Masuda,K., 311
Mathews,G.B., 77
Matlis,E., 38
Matsumura,N., 194
Matthews,C.R., 309
Matusita,K., 38
Matveev,E.M., 74, 75
Mauclaire,J.L., 309
Maurer,D., 190, 192, 311
Maus,E., 192, 253
Mautner,F.I., 402
May,W., 122
Mayer,J., 81
Maza,A.C. de la, 122
Mazur,B., 127, 399, 405, 465, 477
McAuley,M.J., 76
McCall,T.M., 470
McCallum,W.G., 391
McCarthy,P.J., 38, 39
McCoy,D.C., 192, 509
McCulloh,L.R., 188, 189, 196, 308, 388, 404
McDuffee,C.C., 77, 121
McEliece,R.J., 191
McFeat,R.B., 311
McGettrick,A.D., 309
McQuillan,D.L., 461
Mead,D.G., 507
Mead,G.F.Jr., 251
Mennicke,J., 186
Merriman,J.R., 80, 530
Mertens,F., 120, 309, 474, 475
Mestre,J.F., 131, 469, 476
Metsänkylä,T., 461–467, 470, 473
Meyer,C., 398, 399, 460, 468
Meyer,W., 310
Meyer,Y., 76
Mignotte,M., 75
Miki,H., 252, 253, 310, 391
Mills,W.H., 404

Milnor,J., 39, 121
Mines,R., 120
Minkowski,H., 66, 81, 112, 121, 122, 125, 126
Mirimanoff,H., 464
Mishou,H., 390
Mitchell,H.H., 473, 481
Mitsui,T., 395, 400, 402
Miyada,I., 478
Miyake,K., 194, 311, 479
Miyata,T., 187
Miyata,Y., 253
Moine,J.M., 476
Möller,H., 478, 481
Mollin,R.A., 70, 126, 399, 472, 480, 481, 532, 533
Monsky,P., 467
Montes,J., 190
Montgomery,H.L., 73, 74, 396, 397, 403, 462, 463, 468, 470, 473–475, 481
Montouchet,M.N., 480
Moore,M.E., 40
Mordell,L.J., 81, 122, 124, 129, 307, 309, 404, 461, 468, 482
Moree,P., 128
Mori,S., 38
Morikawa,R., 125, 126, 530
Morishima,T., 463, 464
Moriya,M., 120, 191, 193, 403, 476, 477, 480
Moroz,B.Z., 392
Morton,P., 124, 254, 476, 480, 534
Moser,C., 464, 477
Moser,N., 126, 361, 480, 481
Mossinghoff,M.J., 76
Mostowski,A., 404
Motoda,Y., 80, 186
Motohashi,Y., 396
Motzkin,T., 72, 131
Mouhib,A., 194, 477
Moussa,P., 72
Mueller,J., 128
Müller,W., 396, 401, 508, 509
Müntz,W., 81, 389
Murty,M.R., 70, 131, 195, 395, 401, 404, 463, 479
Murty,V.K., 131, 393, 399, 401, 533

Nagata,K., 390
Nagata,M., 191, 251
Nagell,T., 71, 77, 78, 80, 81, 125, 128, 132, 186, 190, 389, 403, 404, 447, 475, 478, 481
Naito,H., 252
Nakagawa,J., 466, 479
Nakagoshi,N., 308, 400, 481
Nakahara,T., 80, 124, 186, 190, 531
Nakamula,K., 125–127, 129
Nakamura,Y., 190, 508
Nakano,M., 38
Nakano,S., 193, 476, 478–480, 532
Nakatsuchi,S., 403
Nakayama,T., 191
Nanda,V.C., 121
Narasimhan,R., 395, 397, 402
Narkiewicz,W., 70, 128, 186, 254, 308, 395, 461, 507–509, 525, 526, 530, 534
Nart,E., 77, 79, 190, 191, 531
Nekovář,J., 465
Nemenzo,F., 475
Netto,E., 308
Neubrand,M., 124, 125
Neugebauer,A., 397, 534
Neukirch,J., 70, 186, 196, 251, 254, 310, 389, 399, 459
Neumann,J.von, 120
Neumann,O., 119, 120, 126, 310, 480
Newman,M., 76, 82, 129, 185, 190, 197, 532
Nguyen-Quang-Do,T., 252
Nicolae,F., 119, 390
Niederreiter,H., 191
Niklasch,G., 117, 128
Nishi,M., 38
Nishizawa,K., 72
Nóbrega,T., 477
Noether,E., 37–39, 163, 186, 188, 253, 308
Nordhoff,H.U., 124
Normandin,F., 75
Northcott,D.G., 39
Notari,C., 75
Novikov,A.P., 127, 398, 460, 465
Nowak,W.G., 401
Nymann,J., 122
Nyul,G., 80

O'Meara,O.T., 39, 131, 307, 308
Odlyzko,A., 81, 82, 394, 397, 401, 403, 471
Odoni,R.W.K., 72, 194, 309, 402, 403, 508, 531
Oesterlé,J., 469
Ogura,H., 470
Oh,J., 466
Oh,S.I., 466

Ohta,K., 192, 480
Okada,T., 187
Okamoto,T., 192
Okazaki,R., 399, 471, 478, 481
Okutsu,K., 78
Olajos,P., 80
Olivier,M., 78, 79, 81, 82, 121, 195, 460, 471
Olson,F.R., 462
Olson,J.E., 489, 507
Omar,S., 397, 534
Onabe,M., 196, 311
Onishi,H., 125
Ono,K., 479
Ono,T., 311, 472
Onuki,M., 310
Oozeki,K., 125
Opolka,H., 71, 308
Oppenheim,A., 130
Ordaz,O., 507
Orde,H.L.S., 461, 532
Ore,O., 77, 79, 123, 185, 186, 190–192, 251, 253, 307
Oriat,B., 78, 193, 476, 477, 479–481
Ortiz,J.J., 77
Osada,H., 478
Ostmann,H.H., 402
Ostrowski,A., 39, 89, 120, 206, 251, 390
Ozaki,M., 466

Pace,F., 507
Pajunen,S., 462
Pall,G., 124, 473, 479, 509
Panaitopol,L., 75
Panario,D., 191
Panella,G., 194
Papick,I.J., 38
Papkov,P.S., 481
Papp,Z.Z., 70, 71, 79, 80
Pappalardi,F., 478
Park,Y.H., 470, 471
Parry,C.J., 78, 125, 192, 404, 470, 479, 480, 509
Patel,P., 254
Pathiaux,M., 75
Pathiaux-Delefosse,M., 76
Patterson,S.J., 309
Pauli,S., 253, 309
Payan,J.J., 77, 78, 80, 126, 190, 191, 193, 252, 311, 404, 464, 477, 480
Pearson,K.R., 308
Pellet,A., 185
Perelli,A., 395
Perlis,R., 71, 310, 390, 532
Perott,J., 124
Perret,M., 121
Perrin-Riou,B., 465
Perron,O., 125, 130
Peterson,B., 78, 404
Petersson,H., 186
Pethő,A., 70, 81, 129, 190, 531
Petr,K., 77
Petridis,Y.N., 463
Pezda,T., 254, 308
Phragmén,E., 399
Pieper,H., 254
Pierce,R.S., 81
Pierce,S., 404
Pink,R., 465
Pinner,C.G., 73
Pintz,J., 467, 468, 473
Pisot,C., 76
Pizer,A., 479
Platonov,V.P., 308
Pleasants,P.A.B., 81, 509
Ploeg,C.van der, 78
Poe,M., 128
Pohst,M., 70, 78–81, 122, 123, 129, 190, 192, 195, 309, 399, 531
Poincaré,H., 399
Poitou,G., 82
Pollaczek,F., 126, 252, 463, 480
Poonen,B., 534
Poorten,A.J. van der, 124, 128
Popken,J., 390
Porusch,J., 308
Potter,H.S.A., 397
Prachar,K., 526
Prapavessi,D.T., 391
Proskurin,N.V., 309
Prüfer,H., 120
Pruis,P., 509
Puchta,J.C., 462
Pumplün,D., 124, 186, 479
Purdy,G., 397
Purkert,W., 120

Quadri,M.A., 38
Queen,C.S., 131, 479
Quême,R., 131
Quer,J., 125, 476
Queyrut,J., 187–189, 393
Quiroz,D., 507

Rabinowitsch,G., 132, 452, 481
Rabung,J.R., 404, 533

Racskó,P., 81
Rademacher,H., 402
Rados,G., 186
Raghavendran,R., 308
Ramachandra,K., 195, 310, 398, 460, 467, 468
Ramakrishnan,D., 393
Ramanathan,K.G., 461
Ranalli,R.R., 470
Ranum,A., 308
Rapoport,M., 195
Rausch,U., 74, 402
Ray,G.A., 76
Rayner,F.J., 251
Razar,M.J., 307, 461
Rédei,L., 124, 130, 476, 479, 481
Rehm,H.P., 481
Reich,A., 390
Reichardt,H., 77, 191, 192, 476, 479
Reidemeister,K., 460
Reiner,I., 40, 186, 189, 475
Reiter,C., 130
Rella,T., 191, 251, 252, 307
Remak,R., 125, 129, 130
Rémond,P., 508, 509
Replogle,D.R., 187
Révesz,S.G., 400
Reyes Sanchez,M.V., 39
Reyssat,E., 76
Rhin,G., 72, 75, 76
Ribenboim,P., 39, 70, 464
Ribet,K.A., 405, 465
Richaud,C., 123
Richert,H.E., 395
Richman,D.R., 78, 460, 470
Richman,F., 120
Rideout,D.E., 461
Rieger,G.J., 122, 309, 400–402
Riele,H.J.J. te, 124
Riemann,B., 306, 389
Riese,U., 309
Rim,D.S., 251
Rio,A., 252
Ritter,J., 126, 189, 251
Robert,A., 310
Robert,A.M., 199
Robert,G., 127, 460, 465
Roberts,D.P., 77, 79, 310, 460
Robertson,L., 80
Robinson,M.L., 469
Robinson,R.M., 51, 72, 76, 529
Roblot,X.F., 253
Rodosskii,K.A., 131, 467
Rogawski,J., 195
Rogers,C.A., 403
Rohrlich,D.E., 391, 397
Rolletschek,H., 130
Rooney,N., 509
Roquette,P., 39, 122, 127, 194, 308, 480
Rosen,M.I., 70, 193, 254, 480
Rosenbaum,K., 254
Rosenblüth,E., 308
Rosiński,J., 508, 531
Ross,K., 511, 514
Rosser,B., 397
Roth,R.L., 404
Rubin,K., 187, 465, 477
Rudin,W., 192, 511
Rudman,R.J., 123, 125
Rumely,R., 72
Rump,S.M., 76
Rush,D.E., 507, 531
Ruthinger,M., 186
Ruzsa,I., 75
Rychlik,K., 251
Rzedowski-Calderon,M., 390

Sairaiji,F., 481
Salce,L., 507
Salem,R., 76
Saltman,D.J., 71, 310
Samet,P.A., 529
Samuel,P., 39, 40, 70, 115, 122, 123
Sanborn,F., 194
Sands,J.W., 129, 393, 462
Sankaranarayana,A., 398
Sansuc,J.J., 308
Saparniyazov,O., 474
Sarbasov,G., 459
Sarges,H., 401
Sarnak,P., 395, 469, 474
Sasaki,R., 481
Sase,M., 479
Satgé,P., 77, 479–481
Sato,K., 191, 393
Saxl,J., 404, 532
Schaal,W., 401
Schaefer,E.F., 534
Schanuel,S., 489, 507
Schappacher,N., 391
Scharaschkin,V., 308
Scharlau,R., 125, 133, 533
Scharlau,W., 192, 311
Scheicher,K., 81
Schenkman,E., 123
Schertz,R., 195, 196, 460, 468, 479, 480

Scheunemann,J., 404
Schilling,O.F.G., 39, 251
Schinzel,A., 49, 71, 73–75, 128, 186, 190, 390, 403, 404, 467, 478, 481, 532
Schipper,R., 192
Schlickewei,H.P., 128, 187
Schmal,B., 78, 404
Schmid,L.H., 309
Schmid,L.P., 402
Schmid,W.A., 507
Schmidt,C.G., 193, 391, 477
Schmidt,F.K., 39, 79, 250
Schmidt,K., 76
Schmidt,W.M., 70, 79, 128, 530
Schmithals,B., 194, 480
Schmitz,T., 130
Schneider,J.E., 308
Schneider,R., 507
Schneiders,U., 122
Scholz,A., 120, 124, 194, 195, 307, 308, 403, 476, 480
Schönemann,T., 251
Schoof,R., 461, 464, 466, 476
Schreiber,J.P., 76
Schreier,O., 403
Schrutka v.Rechtenstamm,G., 461
Schulz-Arenstorff,R., 402
Schulze,V., 403, 404
Schumann,H.G., 194
Schumer,P.D., 401
Schur,I., 71, 79, 81, 130, 186, 307
Schwarz,A., 78
Schwarz,W., 462
Seah,E., 125, 464
Segal,R., 461
Sekiguchi,K., 72
Selberg,A., 394
Selmane,S., 79, 81
Selmer,E.S., 307
Selucký,K., 465
Senge,H.G., 311
Sergeev,E.A., 404
Serre,J.P., 39, 121, 187, 194, 199, 252–254, 311, 394, 398, 403, 405, 531
Setzer,B., 125, 126, 470
Sevilla,A.N., 131
Shafarevich,I.R., 70, 82, 120, 125, 194, 195, 250, 252, 280, 309, 404, 473, 531
Shah,S.I.A., 80
Shah,T., 38
Shanks,D., 121, 402, 477, 480
Shannon,C.E., 507
Shapiro,H.N., 77, 400
Sheingorn,M., 76, 82
Shell,N., 250
Shepherd-Barron,N., 393
Shimizu,K., 481
Shimura,G., 192, 195
Shintani,T., 123, 310, 398, 399, 460, 461
Shirai,S., 193
Shiratani,K., 463, 464, 467
Shokrollah,M.A., 464–466
Shparlinski,I.E., 191
Shyr,J.M., 475, 481
Siegel,C.L., 45, 70, 71, 81, 82, 127–129, 185, 307, 389, 391, 393, 395, 397–399, 404, 461, 462, 467, 468, 474, 508
Sierpiński,W., 104
Silverman,J.H., 75, 129, 254, 391, 534
Sime,P.J., 481
Simon,D., 79
Sinnott,W., 127, 193, 399, 466, 467, 477
Skinner,C.M., 397
Skolem,T., 81, 123, 127, 132, 185
Skopin,A.I., 252, 253
Skoruppa,N.P., 129
Skula,L., 120, 193, 462, 464–466, 507, 531
Slavutskii,I.Sh., 124, 129, 462–465, 473, 479
Śliwa,J., 190, 507–509, 530, 531
Smart,N.P., 128
Smit,B. de, 71, 77, 390, 481, 532, 533
Smith,H.I.S., 69
Smith,J.H., 186, 308
Smith,W.W., 38, 507–509
Smyth,C.J., 71–76, 82, 529
Snaith,V., 189, 465
Snyder,C., 194, 195, 399
Sodaïgui,B., 188, 404
Sokolovskiĭ,A.V., 395, 396, 400
Solderitsch,J.J., 476
Sommer,J., 77
Somodi,M., 390
Sonn,J., 121, 390
Soulé,C., 465
Soundararajan,K., 395, 397, 479
Soverchia,E., 404
Sparer,G.H., 77
Späth,H., 186
Spearman,B.K., 77, 78, 80, 187, 190, 404, 459
Speiser,A., 187, 308, 309, 459
Spencer,J., 71
Sprindzhuk,V.G., 124, 129, 475, 533

Springer,T.A., 307
Srinivasan,A., 122, 481
Srivastav,A., 187
Stankus,E., 474
Stark,H.M., 393, 467–469, 471, 475, 481, 533
Staś,W., 396, 400
Stauffer,R., 187
Steckel,H.D., 307, 460
Steffan,J., 507
Steger,A., 131
Stein,A., 125
Stein,S.K., 507
Steinbacher,F., 309
Steiner,R., 123, 125
Steinig,J., 478
Steinitz,E., 24, 37, 39
Stender,H.J., 125, 480
Stepanov,S.S., 187
Stephens,A.J., 476
Stephens,P.J., 130, 473
Stern,L., 71
Stevenhagen,P., 121, 403, 476, 480, 534
Stewart,C.L., 74, 128
Stewart,I., 70
Stickelberger,L., 79, 185, 193, 477
Stiemke,E., 76, 120
Straus,E.G., 74
Stuart,D., 390
Stuhler,U., 195
Stünzi,M., 479
Sudo,M., 307
Suetuna,Z., 394, 402
Sueyoshi,Y., 253, 480
Sumida,H., 80, 466
Sunley,J.S., 124
Sussman,D., 480
Suzuki,H., 194
Swan,R.G., 39, 185
Swift,J.D., 478
Swinnerton-Dyer,H.P.F., 70, 307
Szegö,G., 72, 75, 402
Szekeres,G., 481
Szydło,B., 400

Takagi,T., 310, 480
Takahashi,S., 194
Takaku,A., 130, 475
Takenouchi,T., 308
Taketa,K., 194
Takeuchi,K., 81
Takeuchi,T., 195
Takhtayan,L.A., 472, 531
Tall,D., 70
Tamagawa,T., 394, 475
Tang,J.E., 78
Tang,S.L., 466
Taniyama,Y., 195, 391
Tannaka,T., 194
Tanner,J.W., 465
Tano,F., 124
Tanoe,F., 80
Tasaka,T., 308
Tate,J., 70, 237, 254, 310, 311, 389, 390, 392, 393, 516, 531
Tateyama,K., 461, 462
Tatuzawa,T., 122, 392, 401, 402, 459, 462, 467, 468, 472, 473
Taussky,O., 121, 186, 190, 194, 195, 197, 480
Taya,H., 466
Taylor,M.J., 70, 126, 187–190, 193, 195, 393, 399, 477
Taylor,R., 393
Teichmüller,O., 250
Terada,F., 194
Thaine,F., 465, 477
Thérond,J.D., 80
Thomas,E., 125
Thompson,J.G., 72
Thompson,R.C., 190
Thompson,W.R., 79, 185
Thue,A., 76
Thurston,H.S., 251
Tijdeman,R., 128
Titchmarsh,E.C., 397
Todd,J., 121
Toepken,H., 186
Tollis,E., 397, 534
Tomanov,G., 310
Torelli,G., 399
Tornheim,L., 77, 190
Torre,P. de la, 460
Touibi,C., 400
Toyama,H., 186
Toyoizumi,M., 399
Tran,N. van, 189
Travesa,A., 252, 460
Trelina,L.A., 79, 80
Tsumura,H., 462
Tunnell,J., 392
Turán,P., 400, 508, 531
Turnbull,H.W., 462
Turunen,R., 77
Tuzuku,T., 191

Uchida,K., 79, 115, 129, 186, 196, 393, 463, 469–471, 478, 480, 529
Uehara,T., 124, 464, 480
Ullom,S., 39, 185, 189, 190, 253, 461
Urazbaev,B.M., 459
Urbanowicz,J., 461, 475
Urbelis,I., 402
Ursell,H.D., 404
Uzkov,A.I., 39

Vaaler,J.D., 73, 399
Valenza,R.J., 508
Vámos,P., 39
Vandiver,H., 462, 464, 465
Varley,R, 72
Värmon,J., 480
Varnavides,P., 130
Vassiliou,P., 192, 459
Vaughan,R.C., 474
Veldkamp,G.R., 115
Vélez,W.Y., 191, 195, 310, 390
Velmin,V.P., 125
Venkataraman,S., 187
Venkov,B.A., 309, 461
Verant,M., 196
Vignéras,M.F., 399
Vijayaraghavan,T., 76, 186
Vila,N., 79
Villa-Salvador,G., 390
Villegas,F.R., 75, 76
Vinberg,E.B., 194
Vinogradov,A.I., 392, 393, 401, 402, 467, 472, 531
Voloch,J.F., 191, 399
Vorhauer,U.M.A., 395
Voronin,S.M., 390
Voronoi,G.F., 77, 125, 185
Vostokov,S.V., 190, 199, 253
Voutier,P., 74
Vulakh,L.Ya., 125

Waall,R.W. van der, 191, 393
Wada,H., 125, 404, 475, 480
Wade,L.I., 38
Wadsworth,A.R., 308
Waerden,B.L. van der, 38, 122, 308, 403
Wagner,C., 469
Wagon,S., 533
Wagstaff,S.S., 465
Wahlin,G.E., 191, 252, 254, 307
Waldschmidt,M., 311, 391
Wales,D., 393
Walfisz,Anna, 402
Walfisz,Arnold, 401, 402, 467, 473
Wall,G.E., 186
Wallisser,R.V., 468
Walter,C.D., 480, 481
Wang,K., 462
Wang,S., 310
Wang,X.D., 393
Wang,Y., 130
Wańtuła,B., 532
Ward,T., 76
Warlimont,R., 402, 474
Warner,S., 250
Wasen,R., 532
Washington,L.C., 70, 127, 193, 251, 254, 309, 404, 405, 461, 462, 464, 466, 467, 470, 476, 477, 480, 531
Watabe,M., 125, 129, 475, 480
Watanabe,S., 79
Waterhouse,W.C., 163, 275, 307–309, 476
Watkins,M., 397, 469
Watt,N., 401
Weber,B.T., 123
Weber,Heinrich, 37, 70, 81, 120, 126, 195, 309, 310, 400, 401, 413
Weber,Helmut, 508
Weber,W., 39
Wegner,U., 79, 192, 403, 508
Weil,A., 70, 154, 186, 310–312, 389–391, 394, 395, 406
Weiler,P., 123
Weinberger,P.J., 121, 127, 131, 404, 468, 474, 475, 478
Weinstein,L., 394, 396
Weisner,L., 186
Weiss,A., 126, 189, 194, 401
Weiss,E., 70
Weiss,M.J., 125, 126
Wellstein,J., 81
Werbiński,T., 395
Westlund,J., 191, 308, 463
Weyl,H., 70, 120
Whaples,G., 21, 120–122, 252, 310
Wheeler,F.S., 469
Whitford,E.E., 124
Wick,B., 533
Wieczorkiewicz,J.K., 396
Wiegand,R., 39
Wiegand,S., 39
Wiegandt,R., 459
Wielandt,H., 390
Wiertelak,K., 400
Więsław,W., 250

Wildanger,K., 80, 122, 128, 129
Wiles,A., 127, 399, 405, 465, 477
Williams,H.C., 70, 77, 124, 125, 389, 399, 461, 464, 470, 472, 475, 476, 481, 532
Williams,K.S., 77, 78, 80, 131, 187, 190, 309, 404, 459–461, 470, 472, 479
Wilson,N.R., 77
Wilson,R.J., 401
Wilson,S., 187
Wilson,S.M.J., 189
Wiman,A., 308
Wingberg,K., 251, 254
Winter,D.J., 187
Wintner,A., 389, 401, 402
Wirsing,E., 395, 402
Witt,E., 250, 307
Wójcik,J., 403, 404
Wolfskill,J., 123
Wolke,D., 474
Wright,D.J., 77, 460
Wright,E.M., 191
Wüstholz,G., 527

Yager,R.I., 465
Yagi,A., 392
Yahagi,O., 121
Yahya,A., 38
Yamagata,S., 251
Yamagishi,M., 252
Yamaguchi,I., 464
Yamamoto,G., 466
Yamamoto,K., 77, 309, 310, 400
Yamamoto,S., 465
Yamamoto,Y., 130, 186, 475, 476, 478, 479
Yamamura,K., 121, 186, 469, 472
Yanagihara,H., 38
Yang,H.S., 471
Yin,L., 477
Yokoi,H., 124, 125, 130, 132, 185, 186, 189, 192, 464, 472
Yokoyama,A., 192, 309, 464, 480
Yoshida,E., 195
Yoshida,H., 393
Yoshino,K.I., 72, 464, 480
Yu,J., 128

Zafrullah,M., 38
Zagier,D., 398, 399, 468, 469, 481
Zaharescu,A., 469, 474
Zahlten,C., 507
Zaimi,T., 76
Zaks,A., 507, 531
Zanardo,P., 507
Zannier,U., 76, 128
Zargouni,H.S., 400
Zariski,O., 39, 40
Zarzycki,P., 402
Zassenhaus,H., 49, 70, 73, 74, 77, 81, 123, 195, 251, 310, 403, 480
Zaupper,T., 481
Zeinalov,B.A., 126
Zelinsky,D., 250
Zelvenskii,I.G., 251
Zhang,L.C., 472
Zhang,M.Y,, 472
Zhang,X., 78, 191, 404, 459, 475, 476
Zheludevich,F.F., 75
Zimmer,H.G., 70
Zimmert,R., 122, 129
Zink,E.W., 194, 479
Zlebov,E.D., 126
Zolotarev,E., 120, 125, 190
Żyliński,E., 190

Subject Index

Abhyankar's lemma, 229
absolute
– discriminant, 52, 135
– extension, 135
– norm, 11
absolutely irreducible element, 486
adele, 286
– class group, 287
– group, 286
– principal, 287
– ring, 286
admissible homomorphism, 324
algebraic
– integer, 43
– number, 43
–– degree, 43
–– minimal polynomial, 43
– number field, 43
almost all integers, 504
ambiguous ideal class, 183
Ankeny-Artin-Chowla conjecture, 124
Archimedean valuation, 17
arithmetically equivalent fields, 390
Artin
– conjecture
–– on L-functions, 392
–– on primitive roots, 308
– L-functions, 392
– reciprocity law, 374
– root number, 393
– symbol, 403
Artin-Hecke zeta function, 394
Artinian ring, 38
associated
– elements, 96
– order, 189
at most tamely ramified prime ideal, 136

Bauerian extension, 376
BC-domain, 254
Bernoulli number, 124
binary quadratic form, 436
block, 488
– irreducible, 488
– length, 488
– unique factorization, 492

canonical number system, 81
capitulation, 194
central ideal class group, 193
character
– even, 267
– Hecke, 323
–– conductor, 328
–– proper, 323
– normalized, 297
– odd, 267
– of a group, 511
– of type (A), 390
– of type (A_0), 391
– primitive, 266
– symplectic, 188
character group, 511
characteristic polynomial, 48
class number, 95
– class number mod I, 95
– narrow, 95
class-field-tower problem, 194
class-group, 92
– narrow, 93
CM-field, 106
codifferent, 146
common non-essential discriminantial divisor, 65
completely ramified prime ideal, 139
complex
– embedding, 44
– valuation, 91
conductor
– of a character, 239, 267
– of a quasicharacter, 240

– of Abelian field, 193, 409
– of Hecke character, 328
conductor-discriminant formula, 459
conjecture
– of Ankeny-Artin-Chowla, 124
– of Artin
–– on L-functions, 392
–– on primitive roots, 308
– of Elliott-Halberstam, 463
– of Hardy and Littlewood, 463
– of Kummer, 462
– of Lehmer, 73
– of Vandiver, 464
conjugated
– elements, 44
– fields, 44
– ideals, 139
content of a form, 120
cross-number, 510
cyclotomic
– polynomial, 162
– unit, 127
– Z_p-extension, 466

Davenport's constant, 489
decomposition
– field, 264
– group, 262
Dedekind domain, 3
degree
– of a function, 394
– of a prime ideal, 137
– of an algebraic number, 43
Delange-Ikehara theorem, 525
Density Hypothesis, 396
density theorem of Chebotarev, 368
derivation, 154
– essential, 155
dicyclic group, 471
different
– of a fractional ideal, 147
– of an element, 150
– of an extension, 147
different theorem, 157
Dirichlet
– class-number formula, 428
– convolution, 405
– density, 344
– series, 525
– unit theorem, 97
discriminant
– absolute, 52, 135
– of a field, 57
– of a module, 57
– of a sequence, 53
– of an element, 53
– regular, 478
– relative, 150
discriminant theorem, 158
divisor group, 93
domain
– Dedekind, 3
– half-factorial, 507
– integrally closed, 5
– Prüfer, 40
dual group, 511

elasticity, 496
element
– absolutely irreducible, 486
– irreducible, 486
– S-integral, 97
elliptic unit, 127
embedding
– complex, 44
– imaginary, 44
– real, 44
equivalent
– factorizations, 492
– ideals, 93
– quasicharacters, 243
– valuations, 16
ERD fields, 472
essential derivation, 155
Euclidean
– domain, 115
– field
–– generalized, 131
–– k-stage, 131
even character, 267
exceptional
– set, 323
– unit, 128
exponent, 18
– of a quasicharacter, 243, 297
exponent ring, 20
extended Richaud-Degert fields, 472
extension
– absolute, 135
– fully ramified, 222
– Kummerian, 176
– relative, 135
– tame, 137, 222
– tamely ramified, 137, 222
– totally ramified, 222
– unramified, 137, 222

– unramified at infinity, 137
– wildly ramified, 222

factorization length, 485
FGC–rings, 39
field
– generalized Euclidean, 131
– irregular, 219
– k-stage Euclidean, 131
– monogenic, 64
– norm-Euclidean, 115
– relatively complete, 251
– solitary, 390
– totally complex, 44
– totally imaginary, 44
– totally real, 44
field discriminant, 57
fields, arithmetically equivalent, 390
finite divisor, 93
finite norm property, 11
first factor, 425
FN-property, 11
Fourier transform, 514
fractional ideal, 1
– principal, 1
Frobenius
– automorphism, 365
– symbol, 365
fully ramified
– extension, 222
– prime ideal, 139
fundamental system
– of S-units, 102
– of totally positive units mod I, 109
– of units, 102
– of units mod I, 109

Gaussian sum, 271
generalized Euclidean field, 131
genus, 443
genus group, 443
Great Riemann Hypothesis, 395
greatest common divisor of ideals, 8
GRH, 395
group
– of ambiguous ideal classes, 183
– of characters, 511
– of finite principal divisors, 93
– of idele classes, 287
– of ideles, 286
– of narrow ray classes mod I, 93
– of ray classes mod I, 93
– of units, 96
– of units of $K_\mathfrak{p}$, 199

Haar
– integral, 514
– measure, 240, 514
half-factorial domains, 507
Hasse
– norm theorem, 307
– principle, 307
Hauptidealsatz, 194
Hecke
– character, 323
-- normalized, 323
-- primitive, 336
-- proper, 323
– theorem on progressions, 400
– zeta-function, 192, 332
Hensel's lemma, 203
HFD, 507
Hilbert class field, 194
Hilbert-Ostrowski theorem, 390
Hilbert-Speiser theorem, 187

ideal
– classes, 36
– fractional, 1
– of the exponent, 20
– principal, 1
ideal theorem, 401
ideals
– conjugated, 139
– equivalent, 93
– equivalent in the narrow sense, 93
– relatively prime, 9
idele, 286
– class group, 287
– group, 286
– principal, 287
imaginary embedding, 44
index
– form, 65
– of a field, 170
– of a number, 58
– of irregularity
-- of a field, 219
-- of a prime, 465
inertia
– field, 264
– group, 232, 263
integer
– algebraic, 43
– of K, 43
– of $K_\mathfrak{p}$, 199

integral
– basis, 55, 211
– closure, 5
– element, 4
integral basis
– normal, 165
integrally closed domain, 5
irreducible
– block, 488
– element, 486
irregular
– field, 219
– prime, 464
irregularity index
– of a field, 219
– of a prime, 465

Jacobi sums, 391

k-stage Euclidean field, 131
Klassenkörperturmproblem, 194
knot group, 307
Krasner's lemma, 206
Kronecker
– class, 403
– constant, 76
– equivalent fields, 403
– limit formula, 398
– theorem, 49
Kronecker-Weber theorem, 280
Kummer's conjecture, 462
Kummerian extension, 176

Langlands program, 195
least common multiple of ideals, 9
Lehmer's conjecture, 73
length
– of a block, 488
– of a factorization, 485
Lenstra constant, 129
Leopoldt's conjecture, 311
locally compact Abelian group, 511

Mahler's measure, 72
maximal order, 81
Mellin transform, 237, 299, 514
minimal polynomial, 43
Minkowski
– constant, 95
– unit, 113, 361
–– strong, 113
module
– Noetherian, 2
– projective, 24
modules
– stably isomorphic, 188
monodromy theorem, 265
monogenic fields, 64
multiplicative family of fields, 418
multiplicative function, 405

narrow class group, 93
narrow class number, 95
– mod$I$, 95
Noetherian
– module, 2
– ring, 1
non-Archimedean valuation, 17
norm, 11, 12
– absolute, 11
– of an element, 48
norm-Euclidean field, 115
normal basis for units, 253
normal integral basis, 165
normal order, 509
normalized
– character, 297
– valuation, 91

odd character, 267
Ono number, 481
order, 81
– associated, 189
– maximal, 81
– of an absolutely irreducible element, 486

p-adic field, 199
$\mathfrak{p}$-adic field, 199
P-adic topology, 19
p-adic topology, 19
p-Eisenstein polynomial, 173
p-independent set, 379
partial zeta-function, 397
Pellet-Stickelberger theorem, 144
periodic point, 254
Piltz divisor problem, 402
Pisot number, 76
Poisson formula, 518
polynomial
– characteristic, 48
– cyclotomic, 162
– Eisensteinian, 173
– reciprocal, 73
positive principal divisor, 93
power bases, equivalent, 80

power integral basis, 64, 211
prime
– irregular, 464
– pseudo-regular, 464
– regular, 464
prime ideal
– at most tamely ramified, 136
– completely ramified, 139
– degree, 137
– fully ramified, 139
– ramified, 136
– split, 139
– tamely ramified, 136
– totally ramified, 139
– unramified, 136
– wildly ramified, 136
prime ideal theorem, 399
primitive
– character, 266
– Hecke character, 336
– quadratic form, 436
– root, 267, 308
principal
– adele, 287
– divisor, 93
– fractional ideal, 1
– idele, 287
– unit, 215
principal ideal theorem, 194
product formula, 91
product of ideals, 1
projective module, 24
Prüfer domain, 40
pseudo-regular prime, 464
PV-number, 76

quasicharacter, 240, 296, 513
– unramified, 240
quasicharacters, equivalent, 243

ramification
– degree of a character, 240
– field, 264
– groups, 232, 263
– index, 136
ramified prime ideal, 136
ray
– class-field, 195
– class-group, 93
– class-group, narrow, 93
real
– valuation, 91
– embedding, 44
– infinite prime divisor, 93
reciprocal polynomial, 73
reduced form, 469
regular
– discriminant, 478
– field, 219
– prime, 464
– set of prime ideals, 344
regulator, 102
relative
– discriminant, 150
– extension, 135
relatively complete field, 251
restricted direct product, 519
restricted minimum condition, 38
Richaud-Degert field, 123
ring
– Artinian, 38
– Noetherian, 1
– of integers of K, 43
– of integers of $K_{\mathfrak{p}}$, 199
– with finite norm, 11

S-integral element, 97
S-unit, 97
Salem number, 76
scalar product of zeta-functions, 392
sci prime, 192
second factor, 425
Selberg class, 394
signature, 44
– group, 44
– map, 44
solitary
– extension, 71
– field, 390
split prime ideal, 139
splitting field, 264
stably isomorphic modules, 188
Steinitz class, 383
Steinitz theorem, 24
Stickelberger ideal, 193, 477
strong approximation theorem, 291
strong Minkowski unit, 113
symplectic character, 188

tame extension, 137
tamely ramified
– extension, 137, 222
– prime ideal, 136
Teichmüller character, 405
theorem
– of Chebotarev, 368

– of Delange-Ikehara, 525
– of Dirichlet, 97
– of Hecke on progressions, 400
– of Hilbert-Ostrowski, 390
– of Hilbert-Speiser, 187
– of Kronecker, 49
– of Kronecker-Weber, 280
– of Pellet-Stickelberger, 144
– of Steinitz, 24
totally complex
– element, 44
– field, 44
totally imaginary field, 44
totally positive number, 44
totally ramified
– extension, 222
– prime ideal, 139
totally real
– element, 44
– field, 44
trace, 48

unique factorization of blocks, 492
unit, 96
– cyclotomic, 127
– elliptic, 127
– exceptional, 128
– principal, 215
unit ideles, 287
unit rank, 102
unit theorem, 97
unramified
– extension, 137, 222
– prime ideal, 136
– quasicharacter, 240

valuation, 16
– Archimedean, 17
– complex, 91
– discrete, 18
– non-Archimedean, 17
– normalized, 19, 91
– real, 91
– trivial, 16
valuation ideal, 20
valuation ring, 20
valuations
– equivalent, 16
Vandiver's conjecture, 464

weak approximation theorem, 21
wildly ramified
– extension, 222
– prime ideal, 136

zeta-function, 243, 299
– of Artin-Hecke, 394
– of Hecke, 192, 332
Z_p-extension, 466

List of Symbols

$(A, B), [A, B]$, 9
$a \equiv b \pmod{I}$, 9
$N(I)$, 11
$\Phi(I)$, 13
R_ν, 19
P_ν, 19
$\mathrm{Ann}(m)$, 33
$\mathrm{Ann}(M)$, 33
$H(R)$, 36

$\deg a$, 43
$\deg_{\mathbb{Q}} a$, 43
$\deg_K a$, 43
R_K, 43
F_i, 44
$r_2(K)$, 44
$r_1(K)$, 44
$Sgn(K)$, 44
Sgn, 44
$a \gg 0$, 44
$N_{L/K}(a)$, 48
$T_{L/K}(a)$, 48
$\overline{|a|}$, 49
$T_n(X)$, 51
$d_{L/K}(v_1, \ldots, v_n)$, 53
$d_{L/K}(a)$, 53
$d_{K/\mathbb{Q}}(M)$, 57
$d(K)$, 57
$M(r_1, r_2)$, 68
$M(a)$, 72
$\epsilon(K)$, 76

$H(K)$, 92
$G(K)$, 92
$P(K)$, 92
$D(K)$, 92
$P_+(K)$, 93
$H^*(K)$, 93
$G_I(K)$, 93
$P_I(K)$, 93
$P_I^+(K)$, 93
$H_I(K)$, 93
$H_I^*(K)$, 93
$h(K), h^*(K), h_I(K), h_I^*(K)$, 95
$U(K)$, 96
$E(K)$, 97
S_∞, 97
$U_S(K)$, 98
$R(u_1, \ldots, u_r)$, 102
$R(K)$, 102
K^+, 105
$U(K, I)$, 109
$U^+(K, I)$, 109
$\mathbb{Z}[G]$, 112
$U_0(K)$, 113
$C(r_1, r_2)$, 121
K_n, 127
$C(K_p)$, 127
$C_0(K)$, 127
$C(K)$, 127

$I(K)$, 135
$i_{L/K}$, 135
$e_{L/K}(\mathfrak{P})$, 136
$f_{L/K}(\mathfrak{P})$, 137
$N_{L/K}(I)$, 140
A^*, 146
$D_{L/K}(I)$, 147
$D_{L/K}$, 147
$d(L/K)$, 150
$\delta_{L/K}(a)$, 150
$\mathfrak{f}_A$, 152
$F_m(X)$, 162
$i(K)$, 170
$i_{L/K}^*$, 180
$H_p(K)$, 181
$Am(L/K)$, 183
$Am_p(L/K)$, 183

$K_\mathfrak{p}$, 199
K_v, 199
$\mathbb{Q}_p$, 199

$R_{\mathfrak{p}}$, 199
Z_p, 199
$U(K_{\mathfrak{p}})$, 199
$e(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, 211
$f(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, 211
$\partial(L/K)$, 211
$D_{L/K}(\omega_1, \ldots, \omega_n)$, 212
$E_1(K)$, 215
$U_m(K)$, 215
$\exp x$, 220
G_i, 232
$X(x)$, 239
$\mathfrak{f}_\chi$, 239
$\mathrm{cond}(q)$, 240
$e(q)$, 243
$Z(f, q)$, 243
$\rho(q)$, 246
$\tau_0(\chi)$, 246

$G_i\mathfrak{P}$, 263
$G(I)$, 266
$\tau_a(\chi)$, 271
$\tau(\chi)$, 271
A_K, 286
A_S, 286
I_K, 286
I_S, 286
U_K, 287
A_0, 287
I_0, 287
$V(x)$, 287
J_K, 287
$C(K)$, 287
$\partial(L/K)$, 292
Q_0, 297
AnJ_K, 297

J'_K, 298
$\tilde{f}(q)$, 299
κ, 299

$\zeta_K(s)$, 313
$\mu_K(I)$, 315
$G(K; S)$, 324
$\zeta(s, \chi)$, 332
$L(s, \chi)$, 338
$s_{\mathfrak{P}}$, 364
$\left[\frac{L/K}{\mathfrak{P}}\right]$, 365
$F_{L/K}$, 365
$P(L/K)$, 376
$(\frac{a}{\mathfrak{q}})_p$, 379
$C_K(L)$, 383
$Cl(M)$, 385

$f(K)$, 409
$X(K)$, 413
$L_d(s)$, 424
h_n^+, 425
h_n^-, 425
$d(f)$, 436
$h(d)$, 439
$\mathfrak{G}(K)$, 443
$g(K)$, 443

$\mathrm{ord}\ a$, 486
$D(A)$, 489
$a_1(A)$, 492
$M(A)$, 494
$\rho(R)$, 496
$\omega_X(I)$, 496
$\omega(I)$, 496

Springer Monographs in Mathematics

This series publishes advanced monographs giving well-written presentations of the "state-of-the-art" in fields of mathematical research that have acquired the maturity needed for such a treatment. They are sufficiently self-contained to be accessible to more than just the intimate specialists of the subject, and sufficiently comprehensive to remain valuable references for many years. Besides the current state of knowledge in its field, an SMM volume should also describe its relevance to and interaction with neighbouring fields of mathematics, and give pointers to future directions of research.

Abhyankar, S.S. **Resolution of Singularities of Embedded Algebraic Surfaces** 2nd enlarged ed. 1998
Andrievskii, V.V.; Blatt, H.-P. **Discrepancy of Signed Measures and Polynomial Approximation** 2002
Angell, T.S.; Kirsch, A. **Optimization Methods in Electromagnetic Radiation** 2004
Ara, P.; Mathieu, M. **Local Multipliers of C*-Algebras** 2003
Armitage, D.H.; Gardiner, S.J. **Classical Potential Theory** 2001
Arnold, L. **Random Dynamical Systems** corr. 2nd printing 2003 (1st ed. 1998)
Arveson, W. **Noncommutative Dynamics and E-Semigroups** 2003
Aubin, T. **Some Nonlinear Problems in Riemannian Geometry** 1998
Auslender, A.; Teboulle M. **Asymptotic Cones and Functions in Optimization and Variational Inequalities** 2003
Bang-Jensen, J.; Gutin, G. **Digraphs** 2001
Baues, H.-J. **Combinatorial Foundation of Homology and Homotopy** 1999
Brown, K.S. **Buildings** 3rd printing 2000
Cherry, W.; Ye, Z. **Nevanlinna's Theory of Value Distribution** 2001
Ching, W.K. **Iterative Methods for Queuing and Manufacturing Systems** 2001
Crabb, M.C.; James, I.M. **Fibrewise Homotopy Theory** 1998
Dineen, S. **Complex Analysis on Infinite Dimensional Spaces** 1999
Dugundji, J.; Granas, A. **Fixed Point Theory** 2003
Elstrodt, J.; Grunewald, F. Mennicke, J. **Groups Acting on Hyperbolic Space** 1998
Fadell, E.R.; Husseini, S.Y. **Geometry and Topology of Configuration Spaces** 2001
Fedorov, Y.N.; Kozlov, V.V. **A Memoir on Integrable Systems** 2001
Flenner, H.; O'Carroll, L. Vogel, W. **Joins and Intersections** 1999
Gelfand, S.I.; Manin, Y.I. **Methods of Homological Algebra** 2nd ed. 2003
Griess, R.L.Jr. **Twelve Sporadic Groups** 1998
Gras, G. **Class Field Theory: From Theory to Practice** 2003
Hida, H. **p-Adic Automorphic Forms on Shimura Varieties** 2004
Ivrii, V. **Microlocal Analysis and Precise Spectral Asymptotics** 1998
Jech, T. **Set Theory** 3rd revised edition 2002
Jorgenson, J.; Lang, S. **Spherical Inversion on SLn (R)** 2001
Kanamori, A.; **The Higher Infinite** 2nd edition 2003
Khoshnevisan, D. **Multiparameter Processes** 2002
Koch, H. **Galois Theory of *p*-Extensions** 2002
Kozlov, V.; Maz'ya, V. **Differential Equations with Operator Coefficients** 1999
Landsman, N.P. **Mathematical Topics between Classical & Quantum Mechanics** 1998
Leach, J.A.; Needham, D.J. **Matched Asymptotic Expansions in Reaction-Diffusion Theory** 2004
Lebedev, L.P.; Vorovich, I.I. **Functional Analysis in Mechanics** 2002
Lemmermeyer, F. **Reciprocity Laws: From Euler to Eisenstein** 2000
Malle, G.; Matzat, B.H. **Inverse Galois Theory** 1999
Mardesic, S. **Strong Shape and Homology** 2000
Margulis, G.A. **On Some Aspects of the Theory of Anosov Systems** 2004
Murdock, J. **Normal Forms and Unfoldings for Local Dynamical Systems** 2002
Narkiewicz, W. **Elementary and Analytic Theory of Algebraic Numbers** 3rd ed. 2004
Narkiewicz, W. **The Development of Prime Number Theory** 2000
Parker, C.; Rowley, P. **Symplectic Amalgams** 2002
Peller, V. (Ed.) **Hankel Operators and Their Applications** 2003

Prestel, A.; Delzell, C.N. **Positive Polynomials** 2001
Puig, L. **Blocks of Finite Groups** 2002
Ranicki, A. **High-dimensional Knot Theory** 1998
Ribenboim, P. **The Theory of Classical Valuations** 1999
Rowe, E.G.P. **Geometrical Physics in Minkowski Spacetime** 2001
Rudyak, Y.B. **On Thom Spectra, Orientability and Cobordism** 1998
Ryan, R.A. **Introduction to Tensor Products of Banach Spaces** 2002
Saranen, J.; Vainikko, G. **Periodic Integral and Pseudodifferential Equations with Numerical Approximation** 2002
Schneider, P. **Nonarchimedean Functional Analysis** 2002
Serre, J-P. **Complex Semisimple Lie Algebras** 2001 (reprint of first ed. 1987)
Serre, J-P. **Galois Cohomology** corr. 2nd printing 2002 (1st ed. 1997)
Serre, J-P. **Local Algebra** 2000
Serre, J-P. **Trees** corr. 2nd printing 2003 (1st ed. 1980)
Smirnov, E. **Hausdorff Spectra in Functional Analysis** 2002
Springer, T.A. Veldkamp, F.D. **Octonions, Jordan Algebras, and Exceptional Groups** 2000
Sznitman, A.-S. **Brownian Motion, Obstacles and Random Media** 1998
Taira, K. **Semigroups, Boundary Value Problems and Markov Processes** 2003
Tits, J.; Weiss, R.M. **Moufang Polygons** 2002
Uchiyama, A. **Hardy Spaces on the Euclidean Space** 2001
Üstünel, A.-S.; Zakai, M. **Transformation of Measure on Wiener Space** 2000
Yang, Y. **Solitons in Field Theory and Nonlinear Analysis** 2001